

BiGuard R1000

智能型双WAN內容管理路由器

用 戶 手 册

版权

版本 2.09，2009 年 7 月

免责声明

Billion 不承担由本手册中提到的产品或软件的使用所引起的责任。既不转让本专利权下的任何许可证也不转让其他任何专利权。Billion 保留在没有任何通知的情况下对本手册内容进行修改的权利。

商标

Mac OS 苹果股份有限公司的注册商标

UNIX 是开放组（Open Group）的注册商标

Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP 是微软公司的注册商标

其他商标是他们各自拥有者的资产

FCC 干扰声明

该产品符合 FCC 标准第 15 部分。 可在以下两种情况下使用：

- 该产品可能不会造成有害的干扰
- 该产品必须能够承受接收到的任何干扰，包括可能造成不期望操作的干扰

该产品经测试已通过 FCC 第 15 部分 B 类数码设备的标准。这些标准被设计用于在商业环境中能够提供合理的保护以防有害的干扰。

如果该产品确实对广播 / 电视信号造成有害的干扰，可以考虑是否关闭。用户可以尝试以下一种或多种方法消除干扰：

- 转动或重置接收天线
- 扩大该产品与信号接收器之间的间距
- 把该产品连接到与信号接收器不同的电路插座上
- 咨询经销商或经验丰富的广播 / 电视信号技术员以寻求帮助

注意：

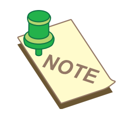
在任何改变或修正未被厂商明确认可前，厂商不对用户在设备上的相关操作负责。

安全信息

BiGuard R1000 是用于长期可靠地在生活中使用。为了您的安全，请务必阅读并且遵照以下的原则和安全警告：

- 在试图安装 BiGuard R1000 以前请详细阅读安装指南。
- BiGuard R1000 是一种复杂的电子设备。不要试图自己打开或维修。打开或移除外壳有可能对您造成高电压和其他风险的伤害。在设备故障的情况下，请立即关掉电源然后送去有资质的服务中心维修。联系您的销售商获取具体的信息。
- 把电源线连上正确的电源。
- 小心谨慎地放置连接线缆以防被行人踩到或绊到。不要把任何东西方在电源线上，不要把电源线放在易被踩到的地方。
- 不要在高湿度或高温度的环境中使用 BiGuard R1000。
- 不要让 BiGuard R1000 和其他设备使用相同的电源。
- 不要在户外使用 BiGuard R1000 和其附件。
- 如果您在墙壁上放置 BiGuard R1000，请确保安装过程中不会损坏到电线，水管或煤气管道。

- 如果没有高峰电压保护，不建议在暴风雨时安装 BiGuard R1000。
- 不要把 BiGuard R1000 暴露在湿气，灰尘或腐蚀性液体中。
- 不要让 BiGuard R1000 靠近水源。
- 确保把线缆连接上正确的端口。
- 不要阻塞 BiGuard R1000 上的通风槽或把它直接暴露在太阳光或其他热源下。过高的温度可能会损坏您的设备。
- 不要在 BiGuard R1000 上放置任何东西。
- 只在 BiGuard R1000 上连接适当的附件。
- 把包装盒放在儿童无法触及的地方。
- 如果要报废该产品，请遵照关于安全处理电子产品的本地相关法规来保护环境。
- 当电源线损坏的时候，请拔去墙壁插座上的路由器电源线。
- 当液体物质渗漏或者溅洒到路由器上的时候，请拔去墙壁插座上的路由器电源线。
- 当路由器掉落或者损坏的时候，请拔去墙壁插座上的路由器电源线。
- 当路由器在建议的用法或环境下不工作的时候，请拔去墙壁插座上的路由器电源线。



NOTE: *访问 Http://cn.billion.com 可获取最新关于 BiGuard R1000 的文档和更新。*

目录

故障排错

BiGuard R1000FAQ

网络基础

技术规格

术语表

保修

插图目录

产品入门

欢迎使用 BiGuard R1000 用户手册。本手册提供所有关于 BiGuard R1000 的产品使用信息，其机架式的设备整合了先进的安全技术，包括虚拟专用网（VPN）和防火墙，让您的网络安全地连接到互联网，不用担心任何入侵攻击。

手册简介

该手册介绍如何安装和操作 BiGuard R1000。请在安装产品以前阅读本手册。

该手册包括以下内容：

- 产品描述，功能和规格
- 硬件安装步骤
- 快速安装向导
- 软件配置信息
- 故障排错
- FAQ
- 网络基础
- 技术规格
- 术语表
- 保修



WARNING: 请参考 安全信息 在 i 页，在安装 BiGuard R1000 之前。

打开 BiGuard R1000 包装

打开 BiGuard R1000 包装 ，检查以下部件：

1. BiGuard R1000 X 1
2. 电源适配器 X 1
3. 保修卡 X 1
4. 软件光盘 X 1
5. 以太网线缆 X 1
6. 安装支架 X 2
7. 安装支架螺丝 X 4

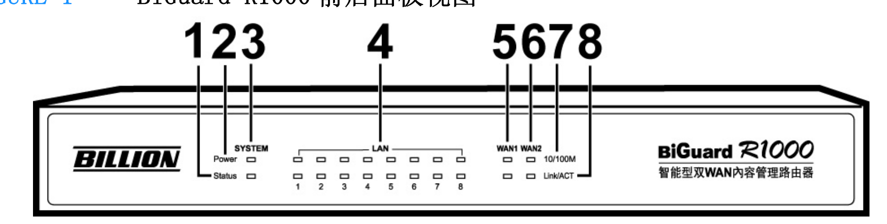


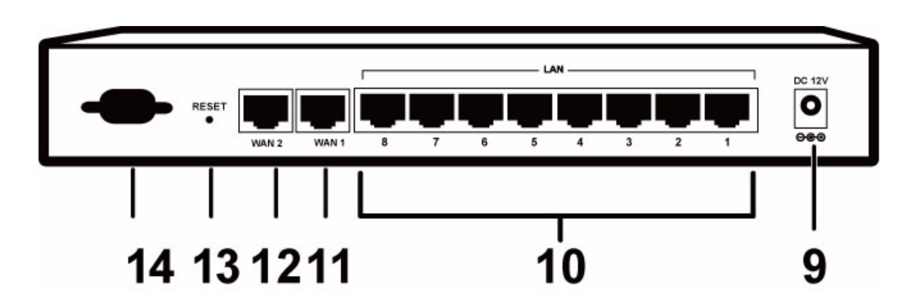
NOTE: *如果有任何部件丢失或者损坏，请将 BIGUARD R1000 重新包装并退回给您的经销商。*

BiGuard R1000 的前后面板视图

图片 1 显示了 BiGuard R1000 的前后面板的组件。

FIGURE 1　　BiGuard R1000 前后面板视图





1. Status LED
   闪烁：设备正在启动
   不亮：设备启动完成
2. Power LED
   亮：电源打开
3. System LED

   系统 LED 包含了 Power LED 和 Status LED
4. LAN 1~8 LEDs
   10/100M
   绿色：以 100Mbps 的速度连接
   不亮：以 10Mbps 的速度连接
   LINK/ACT
   亮：相应端口正在连接 （背面）
   闪烁：有数据在传送和接收
5. WAN1 LED
6. WAN2 LED
7. 10/100 M LED
   绿色：以 100Mbps 的速度连接
   不亮：以 10Mbps 的速度连接
8. LINK/ACT LED
   亮：相应端口正在连接 （背面）
   闪烁：有数据在传送和接收
9. DC 12V 接口
   连接电源适配器
10. LAN 1~8 RJ-45 接口
    使用 UTP 以太网双绞线 (CAT5 或 CAT5e) 连接 PC 到网络
11. WAN1 RJ-45 接口
    10/100M 自适应以太网端口用于连接 xDSL/Cable Modem
12. WAN2 RJ-45 接口
    10/100M 自适应以太网端口用于连接 xDSL/Cable Modem
13. RESET 按钮
    按下 reset 按钮让 BiGuard R1000 恢复到出厂默认配置
14. DB-9/RS232 接口预留槽

网络部署 / 应用程序

这部分的目标是帮助您在网络中正确安装 BiGuard R1000，并介绍不同的组网环境以供您规划公司的网络架构。

在网络中配置 BiGuard R1000 之前，您需要确定您将需要的设备数量和功能类型 （路由器，防火墙或网关）。您需要配置的设备数量取决于子网的数量，网络连接的类型和相连网络的活动情况。

网络环境案例

下面的例子描述了在不同的环境中部署 BiGuard R1000。

多合一解决方案：防火墙，远程访问和 Internet 访问

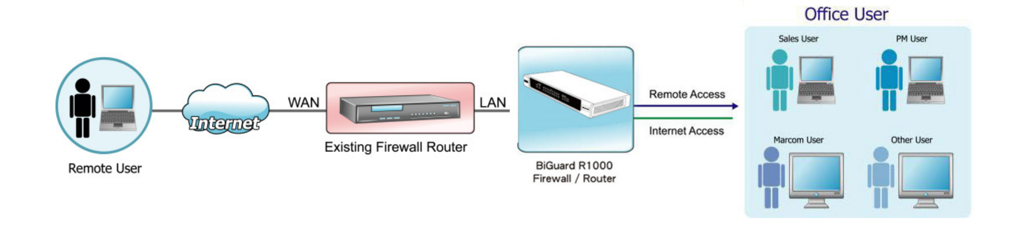
BiGuard R1000 为远程访问公司总部，小型分支机构和中小型企业的网络提供理想的解决方案。BiGuard R1000 还能为公司提供 Internet 访问和防火墙功能。在用户和小型商业机构中的一个典型的设置是让 BiGuard R1000 设备作为一个安全网关连接到 Internet，以提供多合一的安全远程访问和 Internet 访问解决方案。

FIGURE 2　　多合一的解决方案：防火墙，路由器和 Internet 访问

在网关 / 防火墙后面安装

BiGuard R1000 能够放置在任何建好的网络和防火墙后面，以对现有网络造成的最小代价提供安全的远程访问解决方案。

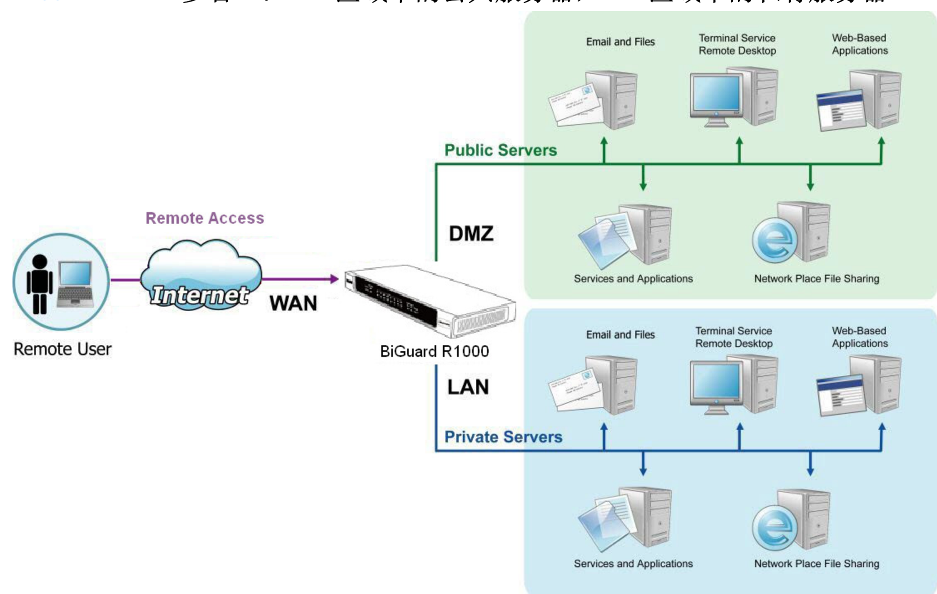
FIGURE 3　　在网关 / 防火墙后面



多合一：DMZ 区域中的公共服务器，LAN 区域中的私有服务器。

以上的 BiGuard R1000 配置是用于远程安全访问，防火墙和 Internet 访问功能。公共服务器放置在 DMZ 区域，可远程安全访问的私有服务器放置在 LAN 区域。

FIGURE 4　多合一：DMZ 区域中的公共服务器，LAN 区域中的私有服务器



策略路由

随着信息量的不断增长 ，人们对 Internet 的通信能力提出了较高的要求。而路由器作为 Internet 通信网络的枢纽和 “交通警察” ，其地位十分重要 ，它的 “工作能力”直接影响到网络的整体性能 ，因此在因特网中 ，路由技术始终处于核心地位。

传统的路由策略都是根据目的地址进行报文的转发。这种机制下，路由器只能为用户提供比较单一的路由方式，它仅解决网络数据的转发问题。而策略路由技术是一种比传统基于目的地更灵活的路由技术 ，它根据数据包的一些特性通过人为定义策略来进行数据包的路由 ，大大提高网络的效率和灵活性 ，它为网络管理者提供了比传统路由协议对报文转发和存储更强的控制能力，使网络管理者不仅仅根据目的地址还能根据协议类型、报文大小、IP 源地址等其它因素来选择转发路径。

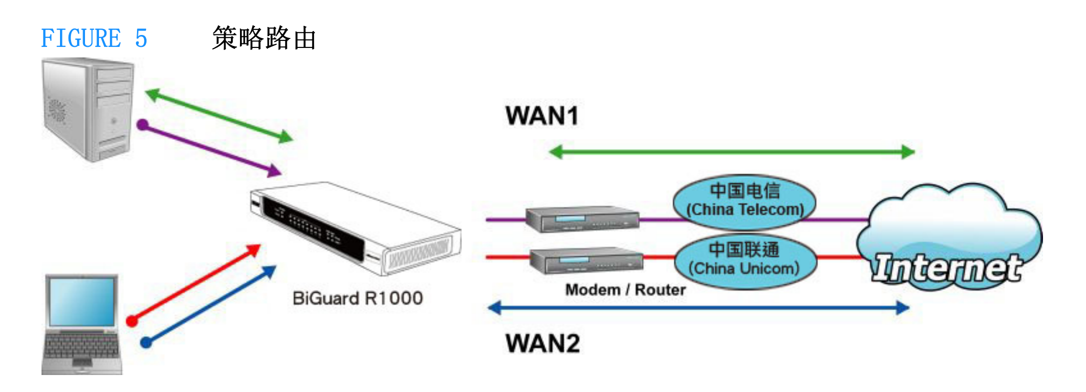
互联网流量工程是避免由于网络资源的非均衡使用而造成网络拥塞、更好地向用户提供 QoS 服务的机构。策略路由是互联网流量工程的重要内容之一，它是根据用户需要向用户提供不同 QoS 服务、满足用户策略要求的重要前提之一。策略路由需要对现有互联网的路由选择协议进行扩充，在选择路由的过程中考虑更多的约束参数 (如带宽、延迟等)，根据链路 (hop) 的资源可用性、服务质量要求及企业 /ISP 的策略选择通路，在源与目的节点之间提供多条满足不同服务质量要求与特定策略的路由。

应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了一个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

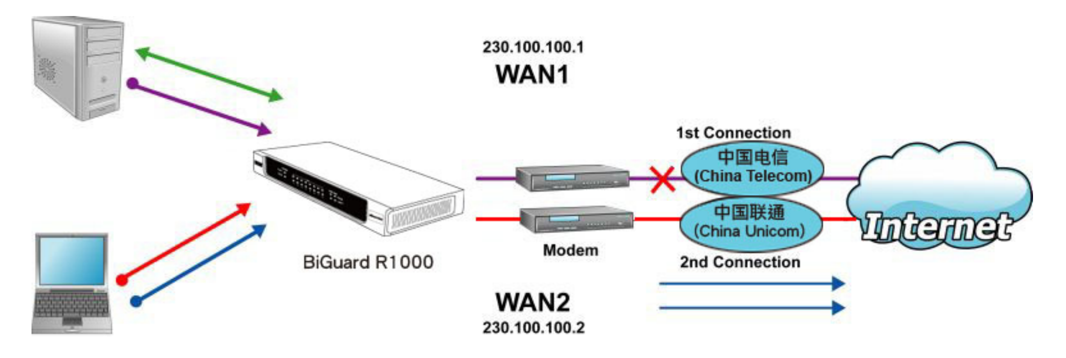
策略路由可以使数据包按照用户指定的策略进行转发。对于某些管理目的，如 QoS 需求或 VPN 拓扑结构，要求某些路由必须经过特定的路径，就可以使用策略路由。例如，一个策略可以指定从某个网络发出的数据包只能转发到某个特定的接口。

策略路由在中国最大的应用莫过于用于中国电信和中国联通的互联互通的问题了，中国特色的网络环境就是南电信，北联通。用户常常在使用 Internet 的时候会发现一个问题：如果用户接入的 ISP 是中国电信，那么访问中国联通的服务器就会比较慢；相反，如果用户接入的 ISP 是中国联通，那么访问中国电信的服务器就会比较慢。人们就想到了接入电信和联通双线路，这种情况下双线路的普及就使得策略路由就有了大的用武之地了！通过在路由设备上添加策略路由包的方式，成功的实现了电信数据走电信，联通数据走联通，这种应用一般都属于目的地址路由！BiGuard R1000 支持双 WAN 接口策略路由功能，一个 WAN 接口连接中国电信，一个 WAN 接口连接中国联通。当用户访问 Internet 的时候，如果目的网络是中国电信，数据包会路由到绑定中国电信的那个 WAN 接口；如果目的网络是中国联通，数据包会路由到绑定中国联通的那个 WAN 接口。这样就很好的解决了跨网访问 Internet 速度慢的问题，有效地提升了访问 Internet 的速度。

FIGURE 5 策略路由



有很多企业通常也用双 WAN 接口连接两条 WAN 线路以保证网络的可靠性，但是往往都是连接到同一个 ISP，所以要么同时状态良好，要么同时出问题。BiGuard R1000 的策略路由功能就可以很好地解决这个问题，大大地提高了网络的可靠性。如果两条 WAN 线路中有一条出现问题，数据包就会自动通过另一条状态良好的 WAN 线路进行发送，而不管目的网络是中国电信还是中国联通。当出现问题的 WAN 线路恢复正常以后，路由器将切换到原先的策略路由模式。



另外，用户还可以自定义策略路由，让指定的数据流路由到不同的 ISP。这样就大大增加了策略路由的灵活性和可扩展性。

内容安全管理

对企事业单位来说，互联网除了可以传送信息、创造商机和联络感情外，还意味着上班时间闲聊打游戏，泄露机密信息，发布非法言论，甚至是巨额资金的非法挪用。

Dynamic Markets Limited 每年会对全球企业员工和 IT 主管进行调查，一方面了解员工的上网习惯，另一方面从 IT 主管的立场来认识企业所面临的网络问题。其中对中国的调查结果令人吃惊：在上班时间，中国员工每周比其他国家多花 7.6 小时来使用即时通讯 (Instant Messenger，IM) 工具、玩游戏、P2P(Peer to Peer，P2P) 下载或在线媒体；中国员工上网下载音乐的时间比

拉美国家高 16%; 上网进入聊天室和玩在线游戏两方面花费的时间分别比其他国家高约 8% 和 12%; 在同为发展中国家的印度，只有 26% 员工在工作场合浏览个人信件，而在中国，这个数字则是 60%!

员工沉溺在互联网带来的诱惑之中，有限的网络带宽资源却被不断蚕食和破坏。包括 BT、电骡、迅雷等带宽资源 “吞噬者”，在资源紧张的前提下，“下载”却是很多员工上班后的第一个工作，来到办公室后，他们自觉地打开了迅雷、电驴、BT 等下载工具，一边娴熟地下载大量的电影和软件，一边抱怨网速太慢、影响其正常工作。在网速问题难以解决的情况下，IT 部门只好申请更多带宽，这无疑给组织增加了运营成本。

网络的内容，例如通过 Web、IM 和文件共享带来的病毒、蠕虫和木马，可以随着鼠标简单点击轻而易举的侵入内网。“堵漏洞、砌高墙、防外攻、防内贼，防不胜防”，防火墙越 “砌”越 “高”，入侵检测越做越复杂，病毒库越来越庞大，身份系统层层设保，却依然无法应对层出不穷网络安全威胁，难道那么多安全产品都是摆设？无论如何豪华的防线，一个漏洞就可以毁灭所有一切。Meta Group 发布研究报告称：“持续增长的安全威胁源自您的员工”。内部人员通过互联网与外部通讯时，可能会引入含有恶意的或者攻击性的内容，如若未能得到监测和控制，这将成为企业的一大隐患。并且充满诱惑的网络资源往往是风险的发源地。

互联网还给泄密提供了便捷的途径。通过邮件、BBS 发帖、FTP、QQ/MSN，员工可以轻而易举地将局域网中的机密信息发给 Internet 上的任何一个人 ; 还有个别员工通过互联网发送非法信息，或在不良的网站上发帖，这些行为也往往给其所在的单位蒙上了不白之冤。更让部分管理者担心的事情也发生了，个别人员利用职位之变，非法盗用企业或单位的流动资金用于炒股或博彩，而恰恰就是网络给他们提供了挪用公款的便利。

内容安全管理是一种约束和规范企业员工遵守工作纪律，提高工作效率的工具，是行政管理的电子化辅助手段。具备内容安全管理功能的路由器无疑对企业网络访问的制度化管理起到了良好的辅助作用。

内容安全管理是不错的网络管理手段，能满足企业网络行为控制的需求！企业网络主要是服务企业业务经营，与企业办公无关的网络应用自然会影响员工工作效率，除了通过公司制度对网络的使用范围进行行政化规定，具备网络行为管理功能的网络设备自然能起到很好辅助效果，做到了不但有制度，而且还有措施。

为了满足企业网络使用中的网络应用管理问题，BiGuard R1000 就提供了内容安全管理功能，BiGuard R1000 可以有效地对网络进行内容安全管理，其主要包括 IM 过滤功能、P2P 过滤功能股票软件过滤功能和视频软件过滤功能，大多数流行的 IM、P2P、股票或视频软件都可以被过滤。与此同时，通过在路由器里进行不同分组内容安全管理设置，以允许一部分人使用 IM、P2P、股票或视频软件 （如老板、管理层）、而有的电脑是不能使用 IM、P2P、股票或视频软件（如财务部门、研发技术部门），对提高企业网络信息化办公效率起到了辅助效果。

FIGURE 6　　内容安全管理

防火墙设定

BiGuard R1000 的内置防火墙功能提供额外的保护，防止破坏性的和非授权的网络访问。防火墙功能是防止入侵者侵入的主要方法。BiGuard R1000 防火墙阻止有害的数据进出私有网络或主机。不仅仅能够提供到 Internet 的安全访问，还能够把公司的内部网络和公共的 Web 服务器分隔开来。除此之外，防火墙还能够保护内部网络，防止非授权的内部网络活动。

包过滤

BiGurd R1000 包过滤可以丢弃或转发特定的数据流，可以有效地控制网络数据流的流向。请参考 启用包过滤 在 78 页。

URL 过滤

BiGuard R1000 的 URL 过滤可以让用户过滤指定的关键字，域名和限制 URL 特性等信息。请参考 配置 URL 过滤 在 81 页。

LAN MAC 过滤

BiGuard R1000 的 LAN MAC 过滤可以对指定 MAC 地址的主机的数据流进行过滤，以决定是否转发该数据流。请参考 配置 LAN MAC 地址过滤 在 83 页。

阻塞 WAN 请求

BiGuard R1000 防火墙能够阻挡 WAN 接口的 PING 请求或所有数据包的请求。请参考 阻塞 WAN 请求 在 86 页。

入侵检测

BiGuard R1000 防火墙功能的入侵监测功能在有非授权访问网络的时候能够向管理员告警并提供入侵防护功能。请参考 配置入侵侦测 在 86 页。

WAN 设定

BiGuard R1000 可以使用静态 IP 地址，PPPoE 协议或者使用 DHCP 客户端动态从 ISP 获得 IP 地址。BiGuard R1000 支持路由模式和 NAT （网络地址转换）模式。请参考 配置 WAN 接口 在 29 页。

DHCP 客户端

通过配置 DHCP 设定，设备能够从 ISP 自动动态地获得 IP 参数。请参考 为 WAN 接口配置 DHCP 客户端 在 11 页。

静态 IP

一个静态的 WAN 连接将根据 ISP 定义的 IP 参数进行配置。若要为 BiGuard R1000 配置静态 WAN 连接，您将需要 ISP 提供一个静态的 IP 地址，子网掩码，默认网关和 DNS 信息。请参考 为 WAN 接口配置静态 IP 在 11 页。

PPPoE

以太网上的点对点协议 （PPPoE）在以太网桢中封装了 PPP 桢。主要用于 Cable Modem 和 DSL 服务。它提供了标准的 PPP 功能，例如认证，加密和压缩。请参考 为 WAN 接口配置 PPPoE 在 12 页。

使用指南

这部分主要介绍如何在 BiGuard R1000 上执行管理任务。快速设置菜单能够帮助您快速设定并启用 WAN。

这部分主要介绍查看配置状态和执行例如改变时间和配置 DHCP 服务器的普通任务。高级管理任务包括映射 MAC 地址，虚拟服务器，静态路由，动态 DNS 和 VLAN 网桥。其他的高级任务包括配置服务质量，防火墙，IM 过滤，P2P 过滤，会话配置和创建系统日志。

这部分还将介绍启用远程访问，固件升级，备份和恢复配置。

快速设置的基本配置

快速设置菜单能让您在 BiGuard R1000 上快速设定并启用 WAN。

登录 BiGuard R1000 Web 管理界面

用 Web 管理界面配置管理 BiGuard R1000。Web 管理界面是基于 web 的接口，您可以通过任何启用 Java 的 Web 浏览器访问。

1. 在 Web 浏览器的地址栏输入默认的 IP 地址：192.168.1.254
   出现登录界面。



2. 输入用户名和密码：
   用户名：admin
   密码：admin
   然后点击**确定**。打开 Web 管理界面显示设备状态。
3. 要注销 Web 管理界面，点击**注销**。弹出**消息**窗口，点击**确定**。





WARNING: 当退出 Web 管理界面的时候，总是使用注销按钮。如果您直接关闭 Web 管理界面没有注销，您将不能在不同的计算机上以相同的用户名登录，直到账户的空闲时间超时。

Web 管理界面导航

点击**菜单栏**打开子菜单。在主界面点击蓝色字体 （表明有链接）打开另外的子菜单或对话框。

FIGURE 7 WEB 管理界面主界面



点击 LOGOUT 直接退出 Web 管理界面，不保存任何更改。点击 RESTART 重新启动 Web 管理界面。在不重启的状态下点击 SAVE CONFIG 把配置文件保存在 flash 存储器中。

用快速设置配置 WAN 参数

这部分介绍如何配置 BiGuard R1000 的基本设定，让网络能够正常运转。下面 WAN 设定的五种方式：

- DHCP 客户端
- 静态 IP
- PPPoE
- PPTP
- Big Pond



NOTE: *BiGuard R1000 有两个 WAN 接口，WAN1 和 WAN2。其配置是完全一样的。下面将以 WAN1 的配置为例。*

为 WAN 接口配置 DHCP 客户端

为 WAN 接口配置 DHCP 客户端可以让 BiGuard R1000 自动获取 IP 地址。

参考下面的配置步骤：

1. 在**菜单栏**中点击**快速开启**。
2. 点击**快速开启 WAN1**。出现**快速开启 WAN1** 的界面。



3. 在**连接方式**下拉选项中选择**自动获得一个 IP 地址**。
4. 点击**应用**保存设定。

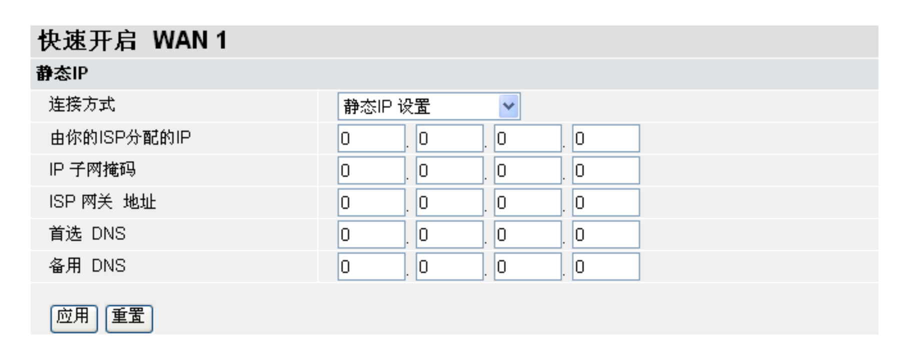
为 WAN 接口配置静态 IP

若要为 WAN 接口配置静态 IP，您需要从 ISP 获得以下信息：

- IP 地址
- 子网掩码
- 网关
- DNS

参考下面的配置步骤 :

1. 在**菜单栏**中点击**快速开启**。
2. 点击**快速开启 WAN1**。出现**快速开启 WAN1** 的界面。



3. 从**连接方式**的下拉选项中选择**静态 IP 设置**。
4. 在**由你的 ISP 分配的** IP 字段中输入 IP 地址。
5. 在 IP **子网掩码**字段中输入子网掩码。
6. 在 ISP **网关地址**字段中输入网关的地址。
7. 在**首选** DNS 字段和**备用** DNS 字段中输入主域名服务器和次域名服务器。
8. 点击**应用**保存设定。

为 WAN 接口配置 PPPoE

若要为 WAN 接口配置 PPPoE，您需要从 ISP 获得以下信息：

- 用户名
- 密码

参考下面的配置步骤：

1. 在**菜单栏**中点击**快速开启**。
2. 点击**快速开启** WAN1。出现**快速开启** WAN1 的界面。



3. 在**连接方式**下拉选项中选择 PPPoE **设置**。
4. 在**用户名**字段中输入用户名。
5. 在**密码**和**重输密码**字段中输入密码。
6. 在**连接**下拉选项中选择**总是连接**或**按需触发**。
   如果您选择了**按需触发**，就需要设定下面的**空闲时间**字段。
7. 在**空闲时间**中选择分钟数。如果您选择了**按需触发**，您将在设定的空闲时间之后自动断开。
8. 点击**应用**保存设定。

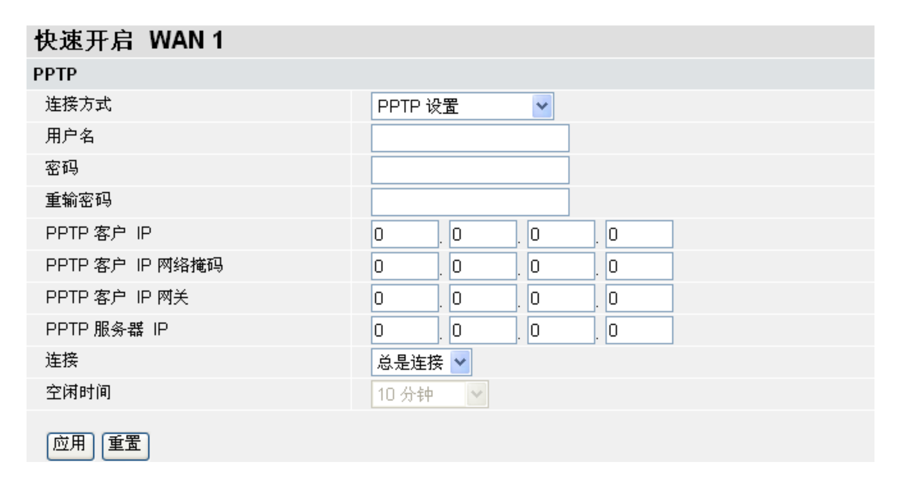
为 WAN 接口配置 PPTP

若要为 WAN 接口配置 PPTP，您需要从 ISP 获得以下信息：

- 用户名
- 密码
- PPTP 客户 IP
- PPTP 服务器 IP

参考下面的配置步骤：

1. 在**菜单栏**中点击**快速开启**。
2. 点击**快速开启** WAN1。出现**快速开启** WAN1 的界面。



3. 在**连接方式**下拉选项中选择 **PPTP 设置**。
4. 在**用户名**字段中输入用户名。
5. 在**密码**和**重输密码**字段中输入密码。
6. 在 **PPTP 客户 IP** 字段输入 PPTP 客户端 IP 地址。
7. 在 **PPTP 客户 IP 网络掩码**字段输入 PPTP 客户端 IP 的网络掩码。
8. 在 **PPTP 客户 IP 网关**字段输入 PPTP 客户端 IP 的网关地址。
9. 在 **PPTP 服务器 IP** 字段输入 PPTP 服务器 IP 地址。
10. 在**连接**下拉选项中选择**总是连接**或**按需触发**。
    如果您选择了**按需触发**，就需要设定下面的**空闲时间**字段。
11. 在**空闲时间**中选择分钟数。如果您选择了**按需触发**，您将在设定的空闲时间之后自动断开。
12. 点击**应用**保存设定。

为 WAN 接口配置 Big Pond

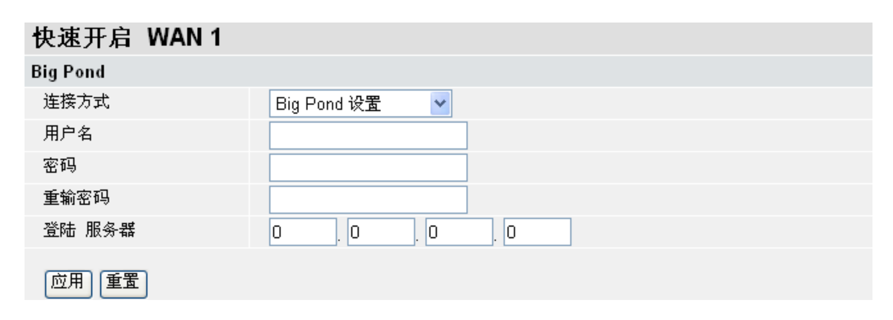
若要为 WAN 接口配置 Big Pond，您需要从 ISP 获得以下信息：

- 用户名
- 密码
- 服务器 IP

参考下面的配置步骤：

1. 在**菜单栏**中点击**快速开启**。

2. 点击**快速开启** WAN1。出现**快速开启** WAN1 的界面。



3. 在**连接方式**下拉选项中选择 Big Pond **设置**。
4. 在**用户名**字段中输入用户名。
5. 在**密码**和**重输密码**字段中输入密码。
6. 在**登陆服务器** IP 字段输入服务器的 IP 地址。
7. 点击**应用**保存设定。

查看配置状态

状态界面能让您查看各种不同的路由器功能的状态。您可以查看设备的概况，包括设备名称，设置当前时间，查看 LAN 和 WAN 的配置信息。您还能够查看 ARP 表，路由表，DHCP 信息。还能够查看系统状态和系统日志。

状态子菜单

在**菜单栏**中点击**状态**打开状态主界面。

FIGURE 8　　查看状态界面

状态		刷新
设备信息		
设备名称	BiGuardR1000	
系统 启动时间	0: 0:25:37 (天:时:分:秒)	
失效切换状态	失效切换（WAN2活动中）	
当前时间	Fri Jul 3 16:24:54 2009	现在同步
私有 LAN MAC 地址	00:11:22:33:44:55	
公有 WAN1 MAC 地址	00:11:22:33:44:56	
公有 WAN2 MAC 地址	00:11:22:33:44:57	
版本信息	2.09	
特征文件版本	1.27 更新于 2009-06-25 13:47:49	
厂商主页	Billion Electric Co.,Ltd.	
LAN		
IP 地址	192.168.1.254	
网络掩码	255.255.255.0	
DHCP 服务器	已启用	
WAN1		
连接方式	无链接	
IP 地址		
网络掩码		
网关		
DNS 服务器		
启动时间		
WAN2		
连接方式	由静态IP设置连接	
IP 地址	172.16.1.67	
网络掩码	255.255.255.0	
网关	172.16.1.254	
DNS	172.16.1.254 172.16.1.240	
启动时间	0: 0:23: 7 (天:时:分:秒)	

设备信息	
设备名称	显示设备的名称，默认是 BiGuard R1000。
系统启动时间	系统启动时间让用户查看系统在线的时间和非预期重启和错误的时间。当断电或者软硬件重置之后，开机时间也会重置。
失效切换状态	显示双 WAN 接口的模式，可以是**策略路由**、**失效切换**或**负载均衡**。
当前时间	显示系统当前时间。

私有 LAN MAC 地址	显示 LAN 接口的 MAC 地址。
公有 WAN1 MAC 地址	显示 WAN1 接口的 MAC 地址。
公有 WAN2 MAC 地址	显示 WAN2 接口的 MAC 地址。
版本信息	显示当前的韧件 （Firmware）版本，在升级以前请检查版本。
特征文件版本	显示当前特征文件的版本。若特征文件为手动升级方式，当特征文件有新的版本时，会有红色字体提示发现新的版本。
厂商主页	显示厂商的主页。
LAN	
IP 地址	显示 LAN 接口的 IP 地址。
网络掩码	显示 LAN 接口的网络掩码。
DHCP 服务器	显示 LAN 接口的 DHCP 服务器状态。
WAN1	
连接方式	显示 WAN1 接口的连接方式。
IP 地址	显示 WAN1 接口的 IP 地址。
网络掩码	显示 WAN1 接口的网络掩码。
网关	显示 WAN1 接口的网关地址。
DNS 服务器	显示 WAN1 接口的 DNS 设定。
启动时间	显示 WAN1 接口的启动时间。
WAN2	
连接方式	显示 WAN2 接口的连接方式。
IP 地址	显示 WAN2 接口的 IP 地址。
网络掩码	显示 WAN2 接口的网络掩码。
网关	显示 WAN2 接口的网关地址。
DNS 服务器	显示 WAN2 接口的 DNS 设定。
启动时间	显示 WAN2 接口的启动时间。

更改时间和时区参数

在**状态**界面中点击**当前时间**。出现**时区**界面。

FIGURE 9　　时区界面

时区

参数	
时区	⦿启用　○禁用
本地 时区 (+-GMT 时间)	(GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi
NTP 服务器 地址	carl.css.gov　india.colorado.edu time.nist.gov　time-b.nist.gov
夏令时	☐自动
重同步周期	1440 分钟

[应用] [取消]

时区	**启动**或**禁用**时区功能。如果您禁用了时区功能，那么其他的部分也将不可用。
本地时区 （+GMT 时间）	从下拉选项中选择您所在位置的时区。
NTP 服务器地址	默认情况下预定义了四个时间服务器地址。您可以更改成您自己的时间服务器。
夏令时	勾选这个复选框能够自动基于你所在位置的夏令时设定更新时间。
重同步周期	输入 BiGuard R1000 的内部时钟与 NTP 服务器同步的周期。

点击**应用**保存设定。

升级特征文件版本

在**状态**界面中，当有新的版本时，会有红色字体提示信息。



状态　[刷新]

设备信息		
设备名称	BiGuardR1000	
系统 启动时间	0: 0:32:13 (天:时:分:秒)	
失效切换状态	失效切换（WAN2活动中）	
当前时间	Fri Jul 3 16:31:30 2009	[现在同步]
私有 LAN MAC 地址	00:11:22:33:44:55	
公有 WAN1 MAC 地址	00:11:22:33:44:56	
公有 WAN2 MAC 地址	00:11:22:33:44:57	
版本信息	2.09	
特征文件版本	1.27 新版本(1.46)	
厂商主页	Billion Electric Co.,Ltd.	

点击红色提示，进入升级界面。

FIGURE 10　特征文件升级界面

手动 升级	
本地版本	1.27
最新版本	1.46
版本说明	146
升级 取消	

点击升级进行版本升级，在升级过程中会显示 Update... 提示。



状态		刷新
设备信息		
设备名称	BiGuardR1000	
系统 启动时间	0: 0:35:20 (天:时:分:秒)	
失效切换状态	失效切换（WAN2活动中）	
当前时间	Fri Jul 3 16:34:37 2009	现在同步
私有 LAN MAC 地址	00:11:22:33:44:55	
公有 WAN1 MAC 地址	00:11:22:33:44:56	
公有 WAN2 MAC 地址	00:11:22:33:44:57	
版本信息	2.09	
特征文件版本	1.27 更新.....	
厂商主页	Billion Electric Co.,Ltd.	

升级完毕后，特征文件版本已显示为最新版本，并显示更新时间。



状态		刷新
设备信息		
设备名称	BiGuardR1000	
系统 启动时间	0: 0:36:55 (天:时:分:秒)	
失效切换状态	失效切换（WAN2活动中）	
当前时间	Fri Jul 3 16:36:13 2009	现在同步
私有 LAN MAC 地址	00:11:22:33:44:55	
公有 WAN1 MAC 地址	00:11:22:33:44:56	
公有 WAN2 MAC 地址	00:11:22:33:44:57	
版本信息	2.09	
特征文件版本	1.46 更新于 2009-07-03 16:34:48	
厂商主页	Billion Electric Co.,Ltd.	



NOTE: *若特征文件为自动升级方式则不需要以上升级步骤。*

更改默认的 LAN 接口 IP 地址

在**状态**界面中点击 **IP 地址**。出现**以太网**界面可以让您对默认的设定进行更改。

FIGURE 11 以太网界面

以太网

参数

IP 地址	192 . 168 . 1 . 254
子网掩码	255 . 255 . 255 . 0
RIP	禁用 ◉ RIP-2B ○ RIP-2M

应用 重置

IP 地址	输入 IP 地址。
子网掩码	输入子网掩码。
RIP	从下拉选项中选择**禁用**，**发送**，**接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 RIP-2B 或 RIP-2M。

点击**应用**保存设定。

DHCP 服务器设定

在**状态**界面中点击 DHCP **服务器**。出现的 DHCP **服务器**界面显示当前的设定。

FIGURE 12 DHCP 服务器界面

DHCP 服务器

参数

DHCP 服务器 功能	⦿启用 ○禁用
IP 池 范围开始	192.168.1. 100
IP 池 范围结束	192.168.1. 199
首选 DNS 服务器	0 . 0 . 0 . 0
备用 DNS 服务器	0 . 0 . 0 . 0
首选 WINS 服务器	0 . 0 . 0 . 0
备用 WINS 服务器	0 . 0 . 0 . 0
网关	0 . 0 . 0 . 0
域名	

应用 重置 主机绑定

BiGuard R1000 可以作为 DHCP 服务器给内部网络分配 IP 地址。如果工作站使用的是静态 IP 地址，可以关闭这个功能。要想了解更多的内容，请参考 配置 DHCP 服务器 在 25 页。

主机绑定

您可以绑定固定的 MAC 地址给工作站以永远分配相同的 IP 地址。绑定的 IP 地址必须是在 DHCP 服务分配的地址范围之外。默认的地址范围是 192.168.1.100 到 192.168.1.199。

FIGURE 13 主机绑定界面

主机绑定

主机绑定列表

名称	
激活	⦿启用 ○禁用
IP 地址	
MAC 地址	

增加 取消 候选

删除

提交

参考下面的步骤绑定固定的 MAC 地址到固定的 IP 地址：

1. 确保您想要绑定的计算机已经连接到设备的 LAN 接口。

2. 在**菜单栏**点击**状态**。在**状态**界面点击 DHCP **服务器**。



3. 点击**主机绑定**。



4. 在**主机名**字段输入计算机名称。
5. 在 IP **地址**字段，输入一个在 DHCP 服务分配的地址范围之外的 IP 地址。其默认范围是 192.168.1.100 到 192.168.1.199。
6. 在 MAC **地址**字段输入计算机的 MAC 地址。
7. 点击**增加**可以添加这个条目，或者也可以点击**候选**，**激活**一个现有条目然后**增加**一个条目。
8. 点击**提交**保存设定。

状态概览

ARP 表

ARP （地址解析协议）是一种 TCP/IP 协议，主要用于获取节点的物理地址。ARP 表界面显示了 IP 地址到 MAC 地址的映射，并给管理员提供了查看系统状态的方法。

在**菜单栏**中点击**状态** →**ARP 表**打开 ARP 表界面。

FIGURE 14 ARP 表界面

ARP 表

IP <> MAC 列表

编号	IP 地址	MAC 地址	接口	静态
1	172.16.1.96	00:26:66:45:88:25	WAN1	no
2	192.168.1.1	00:1A:4B:39:63:70	LAN	no

编号	ARP 条目的编号。
IP 地址	显示计算机的 IP 地址。
MAC 地址	显示计算机的 MAC 地址。
接口	显示 IP 地址相关的 LAN 接口或 WAN 接口。
静态	yes 表明了在 DHCP 服务设定中绑定固定 IP 地址给固定 MAC 地址。 no 表明了在 DHCP 服务设定中没有绑定固定 IP 地址给固定 MAC 地址。

路由表

路由表提供给管理员一个包含当前网络拓扑的数据库，例如转发包的路径。静态和动态路由都将显示在路由表中。

在**菜单栏**中点击**状态** → **路由表**打开**路由表**界面。

FIGURE 15 路由表界面

路由 表

路由 表

编号	目的地	网络掩码	网关/接口	花费
1	192.168.1.0	255.255.255.0	0.0.0.0/ LAN	0
2	172.16.1.0	255.255.255.0	0.0.0.0/ WAN1	0
3	0.0.0.0	0.0.0.0	172.16.1.254/ WAN1	0

编号	路由条目的编号
目的地	显示目标网络的地址段。
网络掩码	显示目标网络的子网掩码。
网关 / 接口	显示路由使用的网关和当前接口的 IP 地址。
花费	显示路由成本，以跳数计算。

DHCP 表

DHCP 表列出了 LAN 接口中通过 BiGuard R1000 的 DHCP 功能分配给工作站的所有 IP 地址。

在**菜单栏**中点击**状态 →DHCP 表**打开 DHCP 表界面。

FIGURE 16　DHCP 表界面

DHCP 表

DHCP IP 分配 表

编号	IP 地址	设备名称	MAC 地址	租期

刷新

编号	显示了 DHCP 条目的编号。
IP 地址	显示了计算机的 IP 地址。
设备名称	显示了计算机的主机名。
MAC 地址	显示了计算机的 MAC 地址。
租期	显示了计算机租用地址的时间。

系统状态

系统状态显示了 BiGuard R1000 的硬件系统的状态。

在**菜单栏**中点击**状态 → 系统状态**打开系统统计界面。

FIGURE 17　系统统计界面

系统 统计

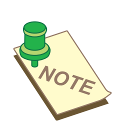
统计

处理器	Intel XScale-IXP425 rev 2 (v5b)
内存总数	30480 kB
剩余内存	8340 kB
虚拟硬盘	1215 kB
CPU状态	2.38%

处理器	显示了 BiGuard R1000 的处理器芯片型号。
内存总数	显示了 BiGuard R1000 的内存总数。
剩余内存	显示了 BiGuard R1000 的剩余内存。
虚拟硬盘	显示了 BiGuard R1000 的虚拟硬盘总数。
CPU 状态	显示了 BiGuard R1000 的处理器使用率。

系统日志

BiGuard R1000 的系统日志功能记录了系统的日志事件。



NOTE: *您可以改变日志中的参数信息。请参考* 日志和 E-mail 通知 *在* 89 *页。*

在菜单栏中点击**状态** → **系统日志**打开**系统日志**界面。

FIGURE 18　　系统日志界面

系统 日志

所有日志

如果你想把日志保存成一个文本文件，右键 这里 选择 “目标另存为...”

显示 所有日志 [刷新] [清除 日志] [发送 日志]

编号	时间	消息		源	目的地
301	Jun 17 15:24:39	SysMan	HTTP Server - Successful login	192.168.1.100	
302	Jun 17 15:25:28	Video	Using the software QQLive	192.168.1.100	119.134.27.181
303	Jun 17 15:27:02	IM	Using the software MSN	192.168.1.100	64.4.9.254
304	Jun 17 15:27:02	IM	Using the software MSN	192.168.1.100	207.46.124.196
305	Jun 17 15:27:07	Game	Using the software MSN Games	192.168.1.100	207.46.73.63
306	Jun 17 15:28:36	SysMan	Save Configurations to flash successfully		
307	Jun 17 15:28:41	SysMan	Save Configurations to flash successfully		
308	Jun 17 15:29:12	P2P	Using the software Thunder	192.168.1.100	123.129.242.168
309	Jun 17 15:29:15	P2P	Using the software Thunder	192.168.1.100	121.9.209.162
310	Jun 17 15:29:15	P2P	Using the software Thunder	192.168.1.100	119.120.94.134

« 第一　‹ 前一个　31 /34　下一个 ›　最后 »

.. 右键 这里 ...	右击这里选择 “目标另存为 ...” 把日志保存下来。
显示	在下拉选项中选择查看的日志类型。
编号	每个日志条目按照从时间顺序排列的序列号。
时间	日志的时间戳。
消息	日志的信息。在选择显示所有的情况下，在信息的前面会出现蓝色字体可以另外选择显示的类型。
源	列出了源 IP 地址。
目的地	列出了目标的 IP 地址。
刷新	点击可以刷新系统日志。
清除日志	点击以清除当前界面的日志。
发送日志	点击以发送当前日志。
第一 / 前一个 / 下一个 / 最后	点击可以定位到相应的位置。

配置 BiGuard R1000

这部分介绍如何配置设备，包括 LAN 接口，WAN 接口。。

另外，您可以执行系统维护和配置，包括配置时区，设定登录密码并重启系统。

最后，您可以配置高级功能，包括配置静态路由，启用动态域名管理系统 （DDNS），设备管理，配置 VLAN 和计划。

配置接口

点击**接口**配置 LAN 接口，WAN 接口和其他高级功能。

配置 LAN 接口

点击 LAN 显示子菜单：**以太网**，**DHCP 服务器**和 **LAN 地址映射**。

<u>配置以太网</u>

以太网界面能让您改变默认的 LAN IP 地址设定。

FIGURE 19 以太网界面

以太网
参数
IP 地址 192 . 168 . 1 . 254
子网掩码 255 . 255 . 255 . 0
RIP 禁用 RIP-2B RIP-2M
应用 重置

IP 地址	输入 IP 地址。
子网掩码	输入子网掩码。
RIP	从下拉选项中选择**禁用**，**发送**，**接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 RIP-2B 或 RIP-2M。

点击**应用**保存设定。

<u>配置 DHCP 服务器</u>

BiGuard R1000 可作为 DHCP 服务器给您的网络分配 IP 地址。如果连在 BiGuard R1000 LAN 接口的工作站使用的是静态 IP 地址，请禁用这个功能。

1. 在 LAN 中点击 **DHCP 服务器**，然后配置相关参数。

FIGURE 20　DHCP 服务器界面

DHCP 服务器

参数

DHCP 服务器 功能	⦿启用 ○禁用
IP 池 范围开始	192.168.1. 100
IP 池 范围结束	192.168.1. 199
首选 DNS 服务器	0 . 0 . 0 . 0
备用 DNS 服务器	0 . 0 . 0 . 0
首选 WINS 服务器	0 . 0 . 0 . 0
备用 WINS 服务器	0 . 0 . 0 . 0
网关	0 . 0 . 0 . 0
域名	

应用　重置　主机绑定

DHCP 服务器功能	如果在网络中手动指定 IP 地址则选择**禁用**。 如果让 BiGuard R1000 在您的网络中自动分配 IP 地址则选择**启用**。
IP 池范围开始	输入分配给 DHCP 客户端的起始 IP 地址。
IP 池范围结束	输入分配给 DHCP 客户端的终止 IP 地址。
首选 DNS 服务器	输入从 ISP 获取的首选 DNS 地址。
备用 DNS 服务器	输入从 ISP 获取的备用 DNS 地址。
首选 WINS 服务器	输入从 ISP 获取的首选 WINS 地址。
备用 WINS 服务器	输入从 ISP 获取的备用 WINS 地址。
网关	分配给 DHCP 客户端的网关地址。
域名	输入域名。如果您使用 BiGuard R1000 代替另一个设备并且不想改变原来的组网环境，输入先前设备的域名。

2. 绑定一个 IP 地址给固定 MAC 地址，点击**主机绑定**。

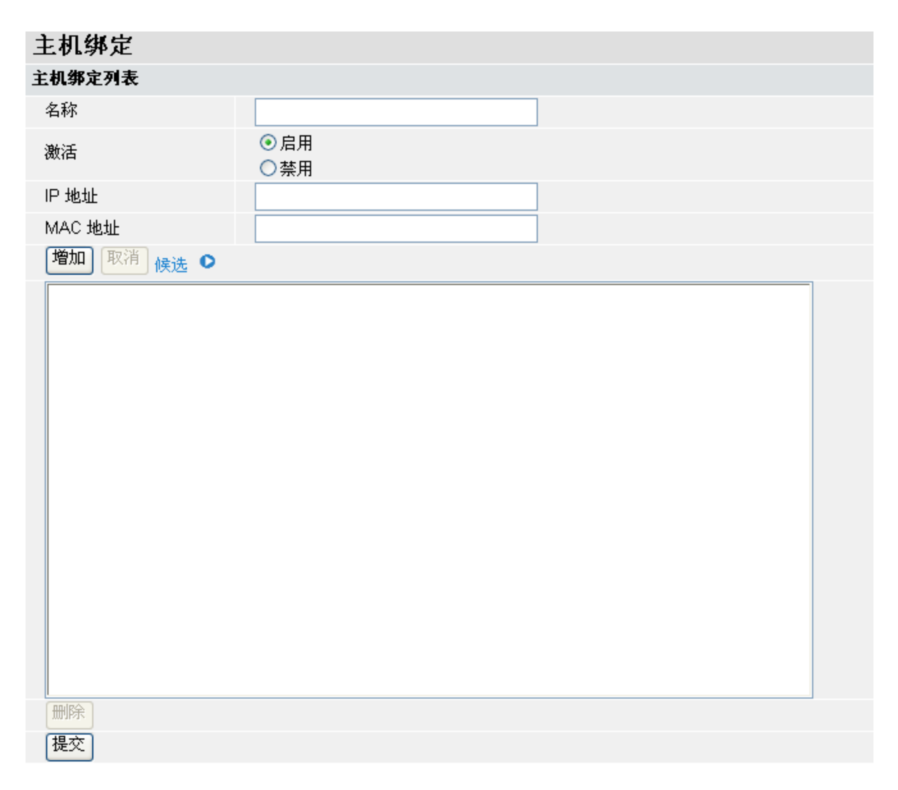
DHCP 服务器

参数

DHCP 服务器 功能	⦿启用 ○禁用
IP 池 范围开始	192.168.1. 100
IP 池 范围结束	192.168.1. 199
首选 DNS 服务器	0 . 0 . 0 . 0
备用 DNS 服务器	0 . 0 . 0 . 0
首选 WINS 服务器	0 . 0 . 0 . 0
备用 WINS 服务器	0 . 0 . 0 . 0
网关	0 . 0 . 0 . 0
域名	

应用　重置　主机绑定

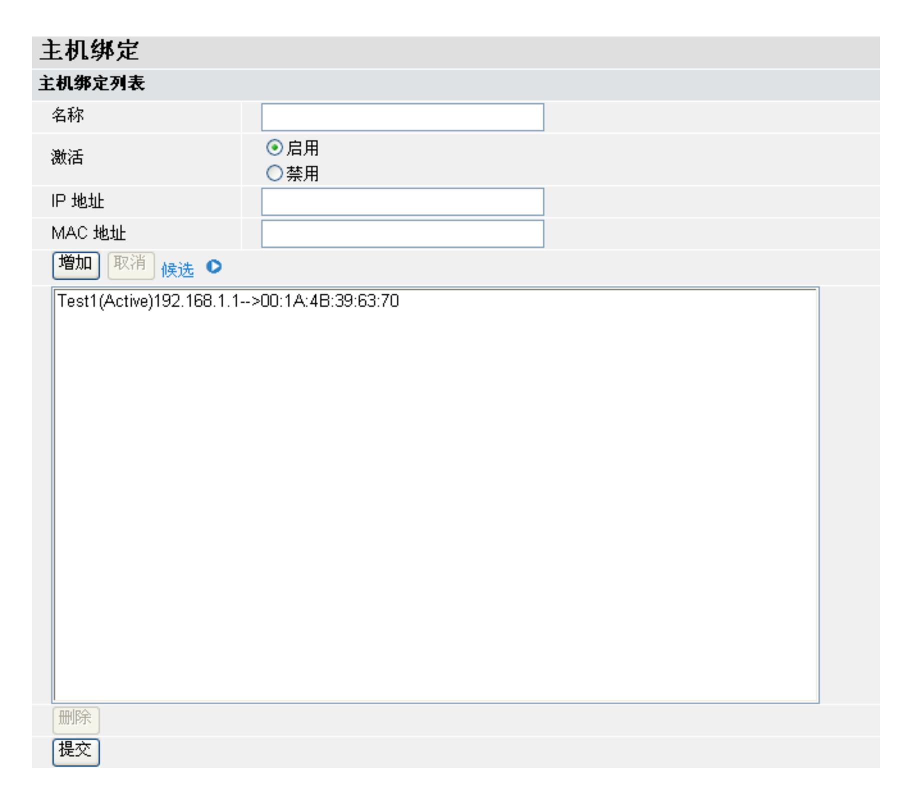
出现下面的界面。



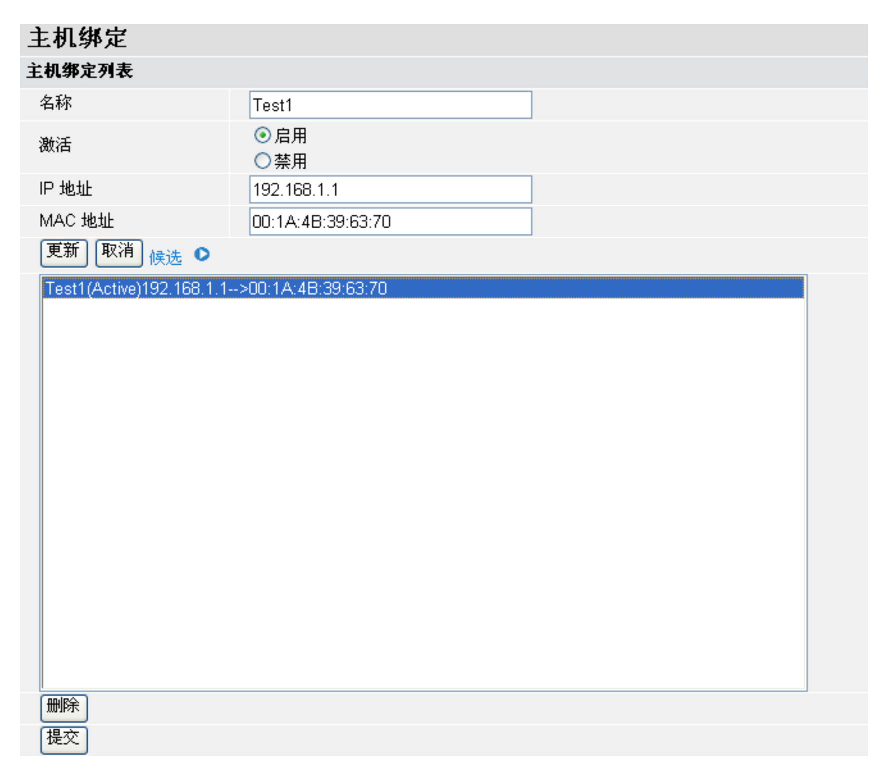
3. 在**名称**字段中输入主机映射条目的名称，选择**启用**该条目，然后在 IP **地址**字段和 MAC **地址**字段输入相应的参数，最后点击**增加**就可以增加一个主机映射条目。
4. 或者点击**候选**选择 LAN 中现有的主机地址。勾选想要选择的主机条目，输入相应的名称，点击**增加**就可以赠加这个主机映射条目。可以点击**都选择**可以选择所有的条目，点击**都清除**可以清除所有选择的条目，点击**关闭**可以退出该界面。



5. 新的条目显示在列表中。



6. 选中该条目，然后可以进行编辑，最后点击**更新**保存设定。如果要删除该条目，可以先选中该条目，然后点击**删除**就可以删除该条目。



7. 点击**提交**保存设定。

配置 LAN 地址映射

LAN 地址映射界面显示了所有配置的新增子网。

FIGURE 21 LAN 地址映射界面

LAN 地址映射				
LAN 地址映射 表				
编号	名称	IP 地址	网络掩码	WAN IP
创建				

编号	LAN 地址映射
名称	子网名称。
IP 地址	子网地址段。
网络掩码	子网的子网掩码。
WAN IP	可以选择是 WAN1 接口的 IP，WAN2 接口的 IP，还是所有 WAN 接口的 IP。

点击**创建**显示增加子网的创建界面。

配置 WAN 接口

这部分介绍如何配置 ISP 设置，带宽设置和 WAN IP 别名。

WAN 指的是广域网。在大多数情况下表示路由器通过 ISP 连接到 Internet。

点击 **WAN**，显示 WAN 接口设置界面，可以配置 ISP 设置，带宽设置和新增 WAN IP 别名。



NOTE: *BiGuard R1000 有两个 WAN 接口，WAN1 和 WAN2。其配置是完全一样的。下面将以 WAN1 的配置为例。*

FIGURE 22 WAN 设置界面

ISP 设置		
WAN 服务 表		
名称	描述	
WAN1	Static IP	编辑
WAN2	DHCP	编辑

ISP 设置

WAN 服务表显示了在 BiGuard R1000 上配置的不同 WAN 连接。

定义路由器如何使用连接方式下拉选项连接 Internet。选择包括使用 DHCP 客户端自动获取 IP 地址，静态 IP，PPPoE，PPTP 或 Big Pond。如果您的 ISP 不使用 DHCP，选择正确的连接方式然后做出相应的配置。配置选项将根据连接方式的不同而不同。

1. 在**菜单栏**中点击**配置 →WAN**。
2. 在 WAN 设置界面，在 WAN1 接口中点击**编辑**，然后出现 WAN1 设置界面。
3. 选择并配置使用的 ISP 设定。

DHCP 客户端

如果您的 ISP 使用 DHCP 协议给您的 WAN 连接分配 IP 地址， 请选择**自动获得一个 IP 地址**。

FIGURE 23　　WAN 设置 DHCP 客户端界面



连接方式	显示当前连接方式。从下拉选项中选择连接方式。
主机名	DHCP 协议的一个参数，用于识别 WAN 接口。
MAC 地址	如果您的 ISP 需要一个预定义的 MAC 地址去访问他们的服务或者允许 BiGuard R1000 能够顺利通过 ISP 的 MAC 过滤器，请选择**你的 ISP 要求你输入 WAN 以太网 MAC**。然后在 MAC 地址字段中输入相应的地址。
DNS	如果您可以自动从 ISP 获取 DNS 参数则不必要选择该选项，如果您的 ISP 不自动分配 DNS 参数信息，你需要勾选**你的 ISP 要求你手工设置 DNS 设置**，然后输入首选 DNS 和备用 DNS。
RIP	从下拉选项中选择**禁用**，**发送**，**接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 RIP-2B 或 RIP-2M。
MTU	MTU （最大传输单元）指的是网络上传输的最大桢长度。如果有桢大于这个数值，就会被切割成小的块。默认的数值能够适应大多数的网络环境。
网络地址转换	选择**启动**可以使用 NAT 模式把内部网络主机的私网 IP 地址 （例如 192.168.0.0 地址段）转换成一个和多个 Internet 公网 IP。选择 NAT 模式给内网用户访问 Internet 提供了额外的安全保护。选择**禁用**可以把路由器置于路由模式，仅仅为地址进行路由。

点击**应用**保存设定。

静态 IP

如果您的 ISP 提供给您静态的 IP，请选择**静态 IP 设置**。

FIGURE 24　　WAN 设置静态 IP 界面

WAN 1
静态IP
连接方式　静态IP 设置
由你的ISP分配的IP　0 . 0 . 0 . 0
IP 子网掩码　0 . 0 . 0 . 0
ISP 网关 地址　0 . 0 . 0 . 0
MAC 地址　你的ISP要求你输入WAN以太网MAC
候选　MAC 地址 00 - 00 - 00 - 00 - 00 - 00
首选 DNS　0 . 0 . 0 . 0
备用 DNS　0 . 0 . 0 . 0
RIP　禁用　RIP-2B　RIP-2M
MTU　1492
网络 地址 转换　启用　禁用
应用　重置

连接方式	显示当前连接方式。从下拉选项中选择连接方式。
由你的 ISP 分配的 IP	输入 ISP 提供的 IP 地址。
IP 子网掩码	输入 ISP 提供的子网掩码。
ISP 网关地址	输入 ISP 提供的网关地址。
MAC 地址	如果您的 ISP 需要一个预定义的 MAC 地址去访问他们的服务或者允许 BiGuard R1000 能够顺利通过 ISP 的 MAC 过滤器，请选择**你的 ISP 要求你输入 WAN 以太网 MAC**。然后在 MAC 地址字段中输入相应的地址。
DNS	如果您可以自动从 ISP 获取 DNS 参数则不必要选择该选项，如果您的 ISP 不自动分配 DNS 参数信息，你需要勾选**你的 ISP 要求你手工设置 DNS 设置**，然后输入首选 DNS 和备用 DNS。
RIP	从下拉选项中选择**禁用**，**发送**，**接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 RIP-2B 或 RIP-2M。
MTU	MTU （最大传输单元）指的是网络上传输的最大桢长度。如果有桢大于这个数值，就会被切割成小的块。默认的数值能够适应大多数的网络环境。
网络地址转换	选择**启动**可以使用 NAT 模式把内部网络主机的私网 IP 地址 （例如 192.168.0.0 地址段）转换成一个和多个 Internet 公网 IP。选择 NAT 模式给内网用户访问 Internet 提供了额外的安全保护。选择**禁用**可以把路由器置于路由模式，仅仅为地址进行路由。

PPPoE

如果您的 ISP 使用 PPPoE 连接方式，请选择 **PPPoE 设置**。

FIGURE 25　　WAN 设置 PPPoE 界面

WAN 1

PPPoE

连接方式	PPPoE 设置
用户名	
密码	
重输密码	
连接	总是连接
空闲时间	无空闲超时
由你的ISP分配的IP	动态 (由你的ISP分配的IP) 固定 (你的ISP要求你输入IP地址) 0 . 0 . 0 . 0
MAC 地址 候选	你的ISP要求你输入WAN以太网MAC MAC 地址 00 . 00 . 00 . 00 . 00 . 00
DNS	你的ISP要求你手工设置DNS设置 首选 DNS 0 . 0 . 0 . 0 备用 DNS 0 . 0 . 0 . 0
RIP	禁用 RIP-2B RIP-2M
MTU	1492
网络地址转换	启用 禁用
延迟启动时间	10 秒

应用 重置

连接方式	显示当前连接方式。从下拉选项中选择连接方式。
用户名	输入 ISP 提供的用户名。
密码	输入 ISP 提供的密码。
重输密码	再次输入 ISP 提供的密码。
连接	在**连接**下拉选项中选择**总是连接**或**按需触发**。 如果您选择了**按需触发**，就需要设定下面的**空闲时间**字段。
空闲时间	在**空闲时间**中选择分钟数。如果您选择了**按需触发**，您将在设定的空闲时间之后自动断开。
由你的 ISP 分配的 IP	如果您的 ISP 自动分配 IP 地址，请选择**动态**。 如果您的 ISP 不自动分配 IP 地址，请选择**固定**，然后输入指定的 IP 地址。
MAC 地址	如果您的 ISP 需要一个预定义的 MAC 地址去访问他们的服务或者允许 BiGuard R1000 能够顺利通过 ISP 的 MAC 过滤器，请选择**你的 ISP 要求你输入 WAN 以太网 MAC**。然后在 MAC 地址字段中输入相应的地址。
DNS	如果您可以自动从 ISP 获取 DNS 参数则不必要选择该选项，如果您的 ISP 不自动分配 DNS 参数信息，你需要勾选**你的 ISP 要求你手工设置 DNS 设置**，然后输入首选 DNS 和备用 DNS。
RIP	从下拉选项中选择**禁用**，**发送**，**接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 RIP-2B 或 RIP-2M。

MTU	MTU （最大传输单元）指的是网络上传输的最大桢长度。如果有桢大于这个数值，就会被切割成小的块。默认的数值能够适应大多数的网络环境。
网络地址转换	选择**启动**可以使用 NAT 模式把内部网络主机的私网 IP 地址 （例如 192.168.0.0 地址段）转换成一个和多个 Internet 公网 IP。选择 NAT 模式给内网用户访问 Internet 提供了额外的安全保护。选择**禁用**可以把路由器置于路由模式，仅仅为地址进行路由。
延迟启动时间	配置完参数以后系统会延迟一段时间再进行拨号，确保系统正常运行。

点击**应用**保存设定。

PPTP

如果您的 ISP 使用 PPTP 连接方式，请选择 **PPTP 设置**。

FIGURE 26 WAN 设置 PPTP 界面

WAN 2

PPTP

连接方式	PPTP 设置
用户名	
密码	
重输密码	
PPTP 客户 IP	0 . 0 . 0 . 0
PPTP 客户 IP 网络掩码	0 . 0 . 0 . 0
PPTP 客户 IP 网关	0 . 0 . 0 . 0
PPTP 服务器 IP	0 . 0 . 0 . 0
连接	总是连接
空闲时间	无空闲超时
由你的ISP分配的IP	⦿动态 (由你的ISP分配的IP) ○固定 (你的ISP要求你输入IP地址) 0 . 0 . 0 . 0
MAC 地址 候选	☐ 你的ISP要求你输入WAN以太网MAC MAC 地址 00 - 00 - 00 - 00 - 00 - 00
DNS	☐你的ISP要求你手工设置DNS设置 首选 DNS 0 . 0 . 0 . 0 备用 DNS 0 . 0 . 0 . 0
RIP	禁用 ⦿ RIP-2B ○ RIP-2M
MTU	1432
网络地址转换	⦿启用 ○禁用

应用 重置

连接方式	显示当前连接方式。从下拉选项中选择连接方式。
用户名	输入 PPTP 的用户名。
密码	输入 PPTP 密码。
重输密码	再次输入 PPTP 密码。
PPTP 客户 IP	输入 PPTP 客户端的 IP 地址。

PPTP 客户 IP 网络掩码	输入 PPTP 客户端 IP 地址的网络掩码。
PPTP 客户 IP 网关	输入 PPTP 客户端 IP 地址的网关地址。
PPTP 服务器 IP	输入 PPTP 服务器的 IP 地址。
连接	在**连接**下拉选项中选择**总是连接**或**按需触发**。 如果您选择了**按需触发**，就需要设定下面的**空闲时间**字段。
空闲时间	在**空闲时间**中选择分钟数。如果您选择了**按需触发**，您将在设定的空闲时间之后自动断开。
由你的 ISP 分配的 IP	如果您的 ISP 自动分配 IP 地址，请选择**动态**。 如果您的 ISP 不自动分配 IP 地址，请选择**固定**，然后输入指定的 IP 地址。
MAC 地址	如果您的 ISP 需要一个预定义的 MAC 地址去访问他们的服务或者允许 BiGuard R1000 能够顺利通过 ISP 的 MAC 过滤器，请选择**你的 ISP 要求你输入 WAN 以太网 MAC**。然后在 MAC 地址字段中输入相应的地址。
DNS	如果您可以自动从 ISP 获取 DNS 参数则不必要选择该选项，如果您的 ISP 不自动分配 DNS 参数信息，你需要勾选**你的 ISP 要求你手工设置 DNS 设置**，然后输入首选 DNS 和备用 DNS。
RIP	从下拉选项中选择**禁用**，**发送**，**接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 RIP-2B 或 RIP-2M。
MTU	MTU （最大传输单元）指的是网络上传输的最大桢长度。如果有桢大于这个数值，就会被切割成小的块。默认的数值能够适应大多数的网络环境。
网络地址转换	选择**启动**可以使用 NAT 模式把内部网络主机的私网 IP 地址 （例如 192.168.0.0 地址段）转换成一个和多个 Internet 公网 IP。选择 NAT 模式给内网用户访问 Internet 提供了额外的安全保护。选择**禁用**可以把路由器置于路由模式，仅仅为地址进行路由。

点击**应用**保存设定。

Big Pond

如果您的 ISP 使用 Big Pond 连接方式，请选择 **Big Pond 设置**。

FIGURE 27 WAN 设置 BIG POND 界面



连接方式	显示当前连接方式。从下拉选项中选择连接方式。
用户名	输入 Big Pond 的用户名。
密码	输入 Big Pond 密码。
重输密码	再次输入 Big Pond 密码。
登陆服务器	输入 Big Pond 服务器的 IP 地址。
MAC 地址	如果您的 ISP 需要一个预定义的 MAC 地址去访问他们的服务或者允许 BiGuard R1000 能够顺利通过 ISP 的 MAC 过滤器，请选择**你的 ISP 要求你输入 WAN 以太网 MAC**。然后在 MAC 地址字段中输入相应的地址。
DNS	如果您可以自动从 ISP 获取 DNS 参数则不必要选择该选项，如果您的 ISP 不自动分配 DNS 参数信息，你需要勾选**你的 ISP 要求你手工设置 DNS 设置**，然后输入首选 DNS 和备用 DNS。
RIP	从下拉选项中选择**禁用，发送，接受**或**兼有**路由信息协议 （RIP）。可以选择的协议包括 **RIP-2B** 或 **RIP-2M**。
MTU	MTU （最大传输单元）指的是网络上传输的最大桢长度。如果有桢大于这个数值，就会被切割成小的块。默认的数值能够适应大多数的网络环境。
网络地址转换	选择**启动**可以使用 NAT 模式把内部网络主机的私网 IP 地址 （例如 192.168.0.0 地址段）转换成一个和多个 Internet 公网 IP。选择 NAT 模式给内网用户访问 Internet 提供了额外的安全保护。选择**禁用**可以把路由器置于路由模式，仅仅为地址进行路由。

点击**应用**保存设定。

配置带宽设置参数

在带宽设置界面可以配置 WAN 接口的出站带宽和入站带宽。

FIGURE 28　　设置 WAN 出入站带宽界面

带宽 设置

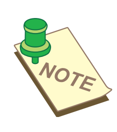
由你的ISP提供的最大带宽

WAN 1	出站 带宽	102400	kbps
	入站 带宽	102400	kbps
WAN 2	出站 带宽	102400	kbps
	入站 带宽	102400	kbps

(*这些带宽设置将会被Qos和负载平衡功能引用*)

应用

WAN1 出站带宽	输入 ISP 提供给 WAN1 接口的最大出站带宽。
WAN1 入站带宽	输入 ISP 提供给 WAN1 接口的最大入站带宽。
WAN2 出站带宽	输入 ISP 提供给 WAN2 接口的最大出站带宽。
WAN2 入站带宽	输入 ISP 提供给 WAN2 接口的最大入站带宽。



NOTE: *这里的数值可以用于 QoS 和负载均衡功能。*

配置 WAN IP 别名

WAN IP 别名界面列出了所有配置的新增 WAN IP。

FIGURE 29　　WAN IP 别名界面

WAN IP 别名

WAN IP 别名 表

编号	名称	IP 地址	接口

创建

点击**创建**，出现**增加 WAN IP** 界面。

WAN IP 别名

增加 WAN IP

名称	
IP 地址	0 . 0 . 0 . 0
接口	⦿ WAN1 ○ WAN2

应用

名称	输入新增 WAN IP 条目的名称。
IP 地址	输入新增 WAN IP 的地址。
接口	选择新增 WAN IP 的 WAN 接口。

配置双 WAN 接口

在这部分您可以设定策略路由，负载均衡或失效切换，出站负载均衡和入站负载均衡，协议绑定。在这个子菜单中有如下选项：一般设置，出站负载均衡，入站负载均衡和协议绑定。

一般设置

点击**一般设置**显示如下选项。



模式	可以选择**策略路由**，**负载均衡**模式或**失效切换**模式。
服务侦测	通过探测网关地址或指定 IP 地址查看 WAN 接口是否存活。此功能只有在**负载均衡**模式中才能启动。
连接决策	输入探测连接失败的次数。
探测周期	输入探测连接的周期。
探测 WAN1	决定探测目标是默认网关或用户指定 IP 地址。
探测 WAN2	决定探测目标是默认网关或用户指定 IP 地址。
可能时回切到 WAN1	如果启动，设备将试图恢复 WAN1，不论 WAN2 是否存活。这就使得 WAN1 成为优先的连接。此功能只有在失效切换模式中才能启动。

点击**应用**保存设定。

如果在**模式**字段选择了**策略路由**，会显示如下选项。

FIGURE 30　　策略路由界面

一般设置

Dual WAN 模式			
模式	⦿策略路由 ○负载均衡 ○失效切换		
WAN端口策略			
默认策略	中国电信	WAN1	
	中国联通	WAN2	
自定义策略	策略1	Disabled	策略更新
	策略2	Disabled	策略更新
WAN端口服务侦测策略			
服务 侦测 (为 负载均衡.)	⦿启用 ○禁用		
连接决策	探测失败后不提供服务满足 3 连接次数.		
探测 周期	每 30 秒.		
探测 WAN1	⦿网关		
	○主机 0.0.0.0		
探测 WAN2	⦿网关		
	○主机 0.0.0.0		
可能时回切到WAN1 (对于失效切换)	○启用		
	⦿禁用		

应用

模式	可以选择**策略路由**，**负载均衡**模式或**失效切换**模式。
默认策略	可以为不同的接口选择不同的运营商，然后设备根据目标 IP 地址判断应该出站的接口。在中国，设备可以自动识别中国电信和中国联通的 IP 地址。
自定义策略	除非在默认策略里面选择 Disabled，否则选择**自定义策略**可以在默认策略的基础上增加自定义的策略。 在策略 1 和策略 2 字段选择相应的 WAN 接口，然后点击**策略更新**可以导入策略。设备可以根据给定的策略判断数据的出站接口。

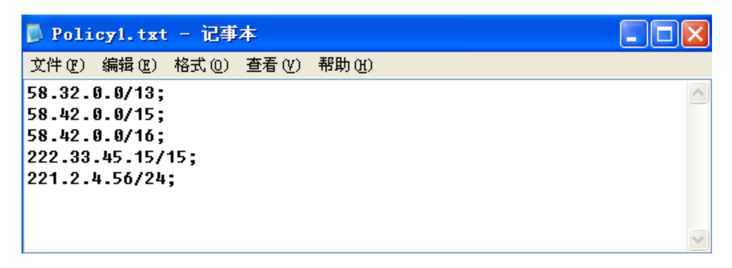
在**策略路由**界面点击**策略更新**。

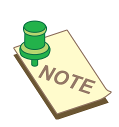
策略更新（自定义策略1）

您可以更新策略到你的设备	
新的策略映像	浏览...

升级

点击**浏览**，找到使用 TXT 编写的策略文件，然后点击**升级**就可以完成策略更新。其 TXT 文件的编写方式如下。策略中的地址段，如 58.32.0.0/13，13 表示前 13 位为网络位，后 19 位为主机位。





1. 必须以分号结尾。
2. 其中，可以只有 IP，如 172.16.1.254，默认掩码为 32。
3. 可以有掩码，如 172.16.1.99/27。
4. 分号前不可以有其他字符，分号后制表符和空格符可以存在。
5. 文件暂时不判断后缀，一般可以用 TXT 格式编写。
6. 文件的大小最大不能超过 1K。

配置负载均衡

负载均衡模式实际上合并了两个 WAN 接口用以增加总体带宽。连接可以被均衡的分配到 WAN1 接口和 WAN2 接口，这样可以充分利用两个 WAN 接口的带宽。当一个 WAN 接口比较慢或者拥塞，连接可能会通过较快的连接进行路由，这样用户就可以获得更多的吞吐量和更少的延迟。

出站负载均衡

对从 WAN1 和 WAN2 接口出去的数据做负载均衡，主要是利用路由器多路径的优点，在可以利用的路径上发送报文。

点击**出站负载均衡**显示如下选项。

FIGURE 31　出站负载均衡界面

Dual Wan

出站负载均衡

负载均衡 策略

基于连接机制
- 由连接平衡 (round robin)
- 由连接平衡 (链接容量权重)
- 比重分配策略 :
- 由流量平衡 (链接容量权重)
- 由流量权重平衡 :

基于IP地址散列机制
- 由链接容量权重平衡
- 由权重平衡 :

应用

BiGuard R1000 上的出站负载均衡有以下两种方式：

1. 基于连接机制
2. 基于 IP 地址散列机制

基于连接机制

根据选定的策略允许源 IP 地址和目标 IP 地址通过 WAN1 和 WAN2。这种机制用于使用中的应用不需要区分不同的 WAN 接口 IP 地址。（一些 Internet 应用需要识别源 IP 地址，例如论坛）

由连接平衡（round robin）	从 WAN1 和 WAN2 接口交替的出去连接，并且连接数基本持平，如果 WAN2 接口出去的连接较少，后续的连接会从 WAN2 出去，以维持平衡状态。
由连接平衡（链接容量权重）	链路容量策略，受 WAN 接口设定的带宽所限制，比如说 WAN1 接口带宽设置为 102400Kbps，WAN2 接口带宽设置为 51200Kbps，那么从 WAN1 和 WAN2 发送出去的连接数为维持在 1：2，也就是说从前一个连接的报文从 WAN1 发送出去，后面的两个连接的报文从 WAN2 发送出去。

比重分配策略	比重分配策略，设置从 WAN1 和 WAN2 出去的连接的百分比。
由流量平衡（链接容量权重）	基于流量的链路容量策略，这种策略也会受 WAN 接口设定的带宽所限制，假定 WAN1 和 WAN2 的带宽设置一样，某个时刻 WAN1 和 WAN2 的连接数比为 3：1，那么后续的连接都会从 WAN2 出去，直到 WAN1 和 WANA2 的连接数接近相同。
由流量权重平衡	基于流量的权重分配策略，这种策略可以由用户指定 WAN1 和 WAN2 的连接数比例，假定用户指定 WAN1 和 WAN2 的比重分配为 2：3，那么在 WAN1 和 WAN2 出去的连接数比就为 2：3。

基于 IP 地址散列机制

根据选定的策略允许源 IP 地址和目标 IP 地址通过指定的 WAN 接口 （WAN1 或 WAN2）。这种机制用于使用中的应用需要区分不同的 WAN 接口 IP 地址。

由链接容量权重平衡	基于流量的链路容量方式，这种策略会受 WAN 接口设定的带宽所限制，假定 WAN1 和 WAN2 的带宽设置一样，某个时刻 WAN1 和 WAN2 的去往目的网络的流量比 3：1，那么后续的流量都会从 WAN2 出去，直到 WAN1 和 WANA2 的流量接近相同。
由权重平衡	这种策略可以由用户指定 WAN1 和 WAN2 的流量比例，假定用户指定 WAN1 和 WAN2 的比重分配为 2：3，那么在 WAN1 和 WAN2 出去的流量比就为 2：3。

点击**应用**保存设定。

入站负载均衡

当企业在内部搭建一些服务器，如 Web 服务器、FTP 服务器等等，提供给 Internet 用户访问。Internet 用户可以通过访问某个 DNS 名来访问这些服务器，那这个部分的配置可以让一部分服务器的流量从 WAN1 出去，其他一部分服务器流量可以去 WAN2 出去，实现流量分流。

点击**入站负载均衡**显示如下选项。

FIGURE 32 入站负载均衡界面

Dual Wan

入站负载均衡

功能	◉启用 ○禁用	
DNS 服务器 1	服务器 设置	编辑
	主机 URL 映射	编辑
DNS 服务器 2	服务器 设置	编辑
	主机 URL 映射	编辑

应用

选择**启用**可以启用该功能。

DNS 服务器主要用来为企业内部服务器做域名解析。

服务器设置

每个 DNS 服务器都会建立一个授权资源记录，在这个资源记录里面需要配置该服务器管理的域名，上级域名服务器，邮件服务器等信息。在**服务器设置**字段点击**编辑**进入 DNS 服务器的配置界面。

FIGURE 33　DNS 服务器配置界面

DNS 服务器 1

SOA	
域名	
* 首选 名称 服务器	
管理员信箱	
序列号	1
刷新 间隔	36000 秒.
重试 间隔	600 秒.
花费时间	86400 秒.
最小 TTL	180 秒.
NS 记录	
* 名称 服务器	
MX 记录	
* 邮件转发服务器	
IP 地址	◉私有 ○公有 0 . 0 . 0 . 0

*: *域将会自动追加的这些字段。*

[应用]

域名	该域名需要向 ISP 申请。如果 ISP 的域名为 xxx.cn，那么申请的域名大概是 yyy.xxx.cn。也就是说需要成为 ISP 域的一个子域，这样做的目的是 Internet 用户可以向 ISP 的 DNS 服务器请求域名解析，进而向该 DNS 服务器请求主机域名解析。
首选名称服务器	配置为自己的主机名称，例如 nsl。
管理员信箱	例如 admin@company.cn
序列号	或者说版本号，每次修改 DNS 服务器上的记录时，序列号都要增加 1。
刷新间隔	该参数是告诉辅 DNS 服务器经过多长时间向主 DNS 服务器请求 DNS 记录列表，以此来更新辅 DNS 服务器上面的 DNS 记录。
重试间隔	该参数是告诉辅 DNS 服务器在第一次请求 DNS 记录列表未得到响应后，继续尝试请求的等待时间。
花费时间	该参数是告诉辅 DNS 服务器，经过多久 DNS 记录就变得不可用了。
最小 TTL	最小存活时间，以秒计算。
名称服务器	指明谁是 yyy.xxx.cn 域的域名解析服务器，这里一般填写自己，例如 nsl.yyy.xxx.cn
邮件转发服务器	为企业用户转发邮件，这里可以填写 IP 地址或者 DNS 名。
IP 地址	指定邮件转发服务器的 IP 地址为企业内部网络的还是公网上的。 • **私有**：企业内部网络使用的 IP 地址。 • **公有**：公网使用的 IP 地址。

点击**应用**保存设定。

主机 URL 映射

主机 URL 映射是为了给企业内部的 Web 或者 FTP 服务器指定一个域名，同时配置服务器为虚拟服务器，虚拟服务器通常可以提供 Internet 用户访问那些放在企业内部网络里面的服务器。配置完服务器设置以后在**主机 URL 映射**字段点击**编辑**进入主机 URL 映射列表界面。

FIGURE 34　　主机 URL 映射列表界面

主机 URL 映射列表

列表

主机 URL	域名	本地 IP 地址	协议	端口范围

创建

点击**创建**可以进入创建主机 URL 映射界面。

主机 URL 映射

一个记录

域名	yyy.xxx.cn
* 主机 URL	
私有 IP 地址 候选	0 . 0 . 0 . 0
协议	任何
端口范围 助手	1 ~ 65535

记录名

* 名称1	
* 名称2	

* : *域将会自动追加的这些字段。*

应用

域名	DNS 服务器所提供的主域。
主机 URL	主机名称 + 主域名成，就成为 Internet 用户访问该服务器的 URL 地址。
私有 IP 地址	企业内部分配给该服务器的 IP 地址，也可以通过点击**候选**进行选择。
协议	该服务器所提供的应用所对应的协议，有以下 5 种： • **TCP**：TCP 协议的应用。 • **UDP**：UDP 协议的应用。 • **ICMP**：ICMP 协议的应用。 • **TCP/UDP**：TCP 和 UDP 协议的应用。 • **任何**：任意的协议，不对协议做特别的指定。
端口范围	应用协议的端口号，也可以通过点击**助手**来进行选择。
记录名	主机名称的别名，主机名称假定为 www，那么可以为主机名称提供最多两个别名，别名 1 是 webserver1，别名 2 是 webserver2。

点击**应用**保存设定。

<u>协议绑定</u>

协议绑定让指定的数据流流经指定的 WAN 接口。点击**协议绑定**显示如下界面。

FIGURE 35　　协议绑定界面

协议绑定

协议绑定 表

编号	接口	源 IP	源 网络掩码	目的 IP	目的 网络掩码	协议	端口 范围

创建

规则决定了指定的 Internet 数据流如何被路由，例如特殊 IP 地址段的数据流被赋予权限访问一个 WAN 接口而不是负载均衡的两个 WAN 接口。



NOTE: *协议绑定条目优先于负载均衡设定。*

1. 点击**创建**可以创建新的规则条目。



接口	选择使用的 WAN 接口，WAN1 或 WAN2。
源 IP 范围	**所有源 IP**：选择所有的源 IP。 **指定源 IP**：选择指定源 IP 地址和子网掩码。
源 IP 地址	如果选择**指定源** IP，那么就输入源 IP 地址。
源 IP 网络掩码	如果选择**指定源** IP，那么就输入源 IP 地址的网络掩码。
目的地 IP 范围	**所有目的** IP：选择所有的目的 IP。 **指定目的** IP：选择指定的目标 IP 地址和子网掩码。
目的地 IP 地址	如果选择**指定目的** IP，那么就输入目标 IP 地址。
目的地 IP 网络掩码	如果选择**指定目的** IP，那么就输入目标 IP 地址的网络掩码。
协议	规则中指定的 Internet 数据流的特定协议。可以选择 TCP，UDP 或**任何**。
端口范围	指定规则的端口范围。（如果需要指定一个端口，在两个方框中输入相同的数值），也可以通过点击**助手**来进行选择。

2. 点击**应用**保存设定。

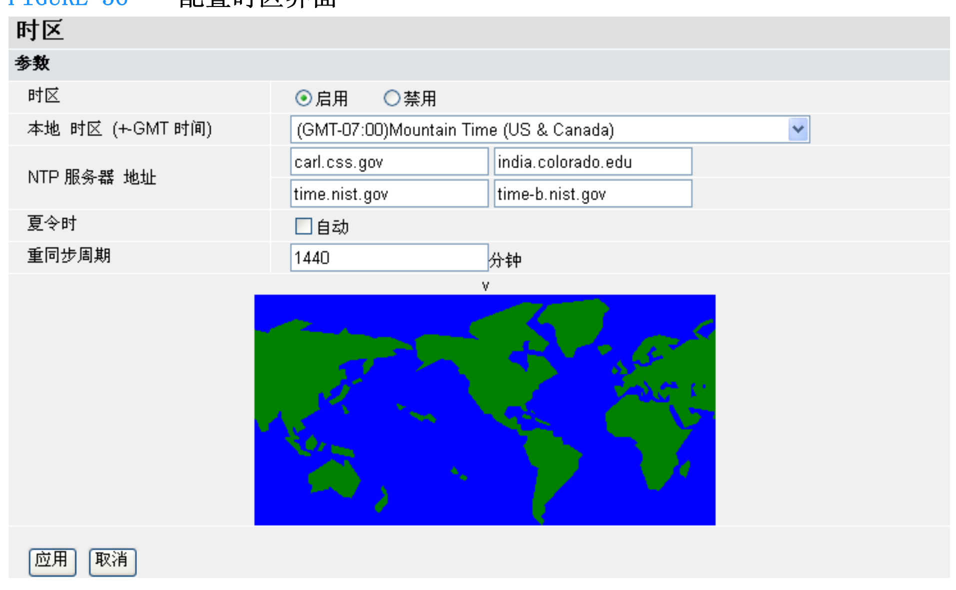
配置系统

点击系统可以设定时区，远程访问，固件升级，备份 / 还原，帐户密码，重启，账户，看门狗，Ping&Tracert 和特征文件升级。

配置时区

1. 点击**时区**打开时区界面。

FIGURE 36　　配置时区界面



时区	**启动**或**禁用**时区功能。如果您禁用了时区功能，那么其他的部分也将不可用。
本地时区 （+GMT 时间）	从下拉选项中选择您所在位置的时区。
NTP 服务器地址	默认情况下预定义了四个时间服务器地址。您可以更改成您自己的时间服务器。
夏令时	勾选这个复选框能够自动基于你所在位置的夏令时设定更新时间。
重同步周期	输入 BiGuard R1000 的内部时钟与 NTP 服务器同步的周期。

2. 点击**应用**保存设定。

启用远程访问

1. 点击**远程访问**启用远程访问功能。

FIGURE 37　启用远程访问界面

远程访问
远程访问 功能
动作　○ 启用 ⦿ 禁用
* HTTPS 端口　443
*：这项设置在你存入闪存并重启路由器后会有效
应用
远程访问 表
编号　IP 地址
创建

远程访问功能	
动作	选择启用可以允许远程访问。
HTTPS 端口	可以自定义 HTTPS 端口用于远程访问，默认端口是 443。
远程访问表	
编号	远程访问规则条目的编号。
IP 地址	允许远程访问的 IP 地址。

2. 点击**创建**进入配置远程访问主机的界面。

FIGURE 38　配置远程访问主机界面

远程访问
你可以对这台网络设备远程管理 (HTTPS).
允许远程访问由　⦿ 每人 (每人)
○ 只这台PC:
○ 来自这个子网的PC:
应用

每人	允许任何人访问该设备。
只这台 PC	只允许指定的一台 PC 访问该设备。
来自于这个子网的 PC	只允许指定子网的 PC 访问该设备。

3. 点击**应用**保存设定返回启动远程访问界面。



4. 点击应用**保存**设定。



WARNING: 如果允许远程访问控制，建议您配置指定的 IP 地址，以供管理员使用。

升级 BiGuard R1000 软件版本

1. 下载软件包，保存在指定的位置。
2. 点击**固件升级**可以升级设备的软件。

FIGURE 39 固件升级界面



3. 点击**浏览**找到需要升级的软件版本。
4. 点击**升级**进行软件版本升级。
5. 注意不要在升级的时候进行任何操作。



WARNING: 在完全升级好软件版本的情况下才可以使用 BiGuard R1000。在升级期间的任何中断 （包括停电）可能致使设备不能正常工作。

6. BiGuard R1000 将在升级完成的时候自动注销。如果要更改其他设置，请再次登录。

备份 / 还原配置

您可以通过**备份 / 还原**为灵活的网络管理备份和还原不同的配置。点击**备份 / 还原**打开备份 / 还原界面。

FIGURE 40 备份 / 还原界面

备份 / 复原

允许你备份配置设置到你的计算机，
或从你的计算机复原配置信息。

备份 配置

备份配置到你的计算机。

备份

还原 配置

配置 文件 浏览...

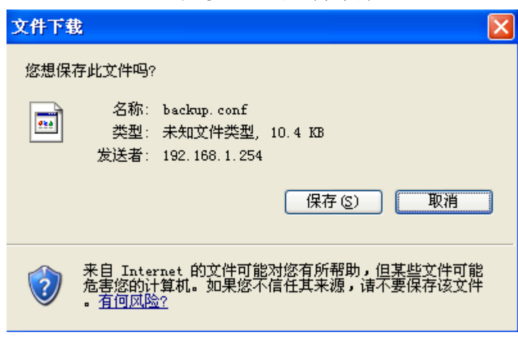
"复原"将会覆盖当前配置并重启设备 如果你想保持当前配置请使用先使用"备份"来保存当前配置。

还原

备份配置

点击**备份**就开始备份配置了。您将被提示在电脑上保存配置文件。

FIGURE 41 备份配置文件确认



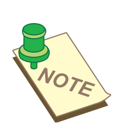
还原配置

参考以下步骤还原配置：

1. 点击**浏览**找到将要还原的配置文件。
2. 点击**还原**开始还原配置文件。



3. 在设备还原以后才能进行操作。还 BiGuard R1000 将在还原完成的时候自动注销。如果要更改其他设置，请再次登录。



WARNING: 您必须点击屏幕右下角的 Sava Config 按钮把当前的配置文件保存在 Flash 存储器中。请参考 在 91 页。
WARNING: 要还原配置文件，您必须已经有一个备份好的配置文件。

重新启动系统

1. 点击**重启**可以看到重新启动的界面。

FIGURE 42 重启界面

重启	
重启后，请等待几秒钟来使系统重启	
重启路由器使用	◉ 当前 设置 ○ 出厂设置
[重启]	

2. 您可以选择下面两种选项重新启动路由器：

- 当前设置：重新启动路由器，不保存当前配置。
- 出厂设置：重新启动以后使用出厂默认配置。

3. 点击**重启**就可以重启路由器。

帐户

点击**帐户**可以更改访问 BiGuard R1000 管理界面的用户名和密码。

FIGURE 43 更改密码界面

帐户	
参数	
帐户	********
确认帐户	********
密码	••••••••
确认密码	••••••••
⚠ 注意: 帐户最大为10个字符, 密码最大为32个字符	
[应用] [重置]	

在**帐户**和**确认帐户**字段中输入新的帐户名称，在**密码**和**确认密码**字段中输入新密码。然后点击**应用**保存设定。

看门狗

点击**看门狗**可以看到设置看门狗的界面。

看门狗
参数
看门狗 ☐启用
自动重启 ☐启用 0 (小时): 0 (分钟)
应用

看门狗	选择**启用**可以启用看门狗功能。
自动重启	选择**启用**可以启用自动重启功能，并设置自动重启时间。

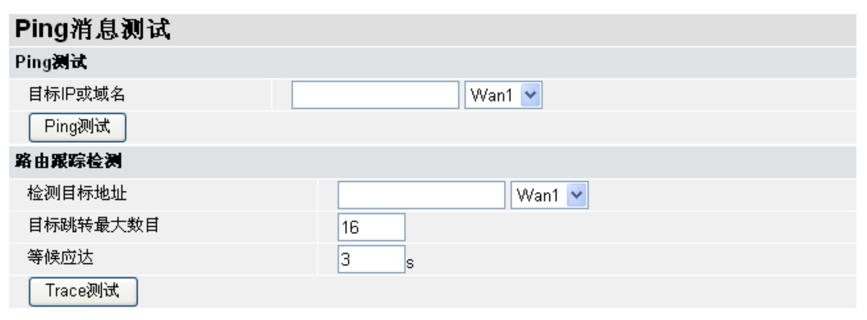
点击**应用**保存设定。

Ping&Tracert

您可以通过该功能对现有网络进行诊断。点击 Ping&Tracert 打开 **Ping 消息测试**界面。

可以选择以下两种诊断方式：

- Ping 测试：用 Ping 工具可以测试网络是否连接及网络延时，相当于操作系统中的 Ping 命令。
- 路由跟踪检测：用 Trace 工具可以检测路由的状况，相当于操作系统中的 Tracert 或 Traceroute 命令。



Ping 测试	输入 Ping 测试的目标 IP 地址或 DNS 名，然后选择数据包出站接口，WAN1 或 WAN2，点击 **Ping 测试**就可以进行测试。
路由跟踪检测	输入检测的目标地址，然后选择数据包出站的接口，WAN1 或 WAN2，选择路由最大跳数和等候应答时间，然后点击 **Trace 测试**就可以进行测试。

特征文件升级

由于 IM 以及 P2P 软件的版本不断升级，它们的特征码也随之变化，因此需要不断去更新特征文件，以达到上网行为管理的目的。

可以选择以下两种升级方式：

- 自动升级：设置升级间隔时间，就可以自动去更新。
- 手动升级：有新的特征文件版本时，通过 Email 通知用户。用户可以根据需要去选择要升级的版本。

特征文件升级	
当前版本	1.24
升级方式	自动 手动
时间设置	每月 1st 00:00
电子邮箱	
完成	

当前版本	显示当前特征文件的版本。
升级方式	选择自动或者手动升级方式。
时间设置	系统会按照设定的时间去检查特征文件是否有新的版本。
电子邮箱	当特征文件有新版本时，会自动发邮件通知用户。

配置虚拟服务器

点击**虚拟服务器**查看虚拟服务器列表和参数。

FIGURE 44　　虚拟服务器参数界面



配置 DMZ

启用 DMZ 后，可以让外部用户访问指定 DMZ IP 地址上所有的端口。

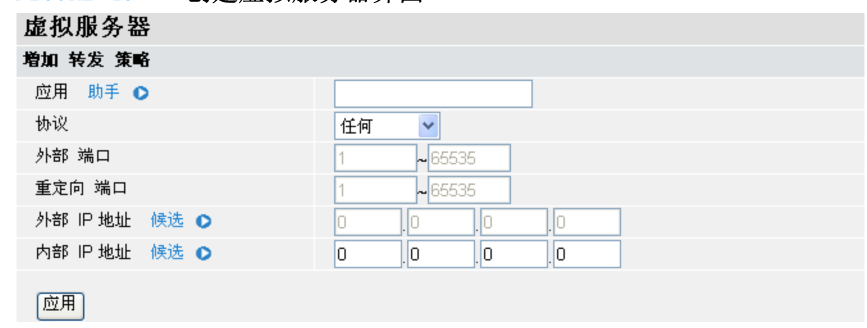
1. 选择**启用**可以启用 DMZ 功能。
2. 在 **DMZ IP 地址**字段中输入内部应用服务器的 IP 地址，也可以点击**候选**进行选择。
3. 点击**应用**保存设定。

配置虚拟服务器

<u>创建虚拟服务器参数</u>

1. 点击**创建**增加一个虚拟服务器条目。

FIGURE 45　创建虚拟服务器界面



应用	输入虚拟服务器转发的应用名称。
协议	该应用使用的协议，可以选择 TCP，UDP，ICMP，TCP/UDP 和**任何**。
服务	从下拉选项中选择服务网络对象。
外部端口	给用户提供从 WAN 接口访问的端口。例如 HTTP 服务的 80 端口。
重定向端口	内部应用服务器的实际端口。例如实际端口是 8080，路由器就会把 WAN 接口上访问 80 端口的数据包映射到内部应用服务器的 8080 端口。
外部 IP 地址	点击**候选**可以选择 WAN1，WAN2 或者所有 WAN 接口的 IP 地址。
内部 IP 地址	内部应用服务器的实际 IP 地址。可以点击**候选**进行选择。

2. 点击**应用**保存设定。

编辑虚拟服务器参数

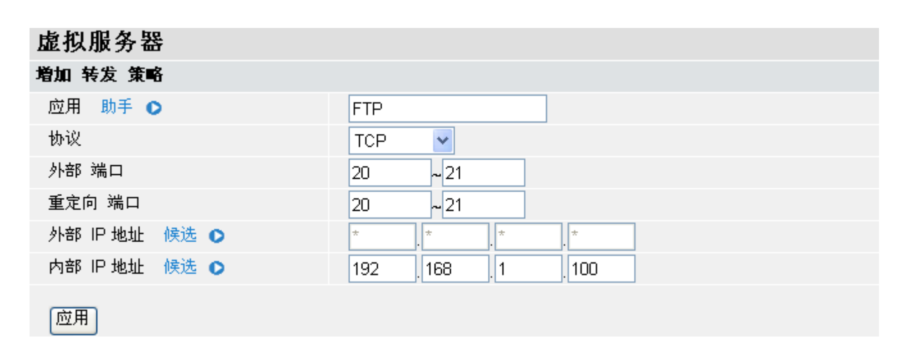
参考以下步骤编辑虚拟服务器条目：

1. 在虚拟服务器参数界面中，点击**编辑**。

FIGURE 46　编辑虚拟服务器参数界面



以下界面显示了虚拟服务器条目的参数。



虚拟服务器

增加 转发 策略

应用 助手	FTP
协议	TCP
外部 端口	20 ~21
重定向 端口	20 ~21
外部 IP 地址 候选	* . * . * . *
内部 IP 地址 候选	192 . 168 . 1 . 100

应用

2. 编辑虚拟服务器参数。
3. 点击**应用**保存设定。

<u>删除虚拟服务器参数</u>

参考以下步骤删除虚拟服务器条目：

1. 在虚拟服务器参数界面中，点击**删除**。

FIGURE 47 删除虚拟服务器条目界面



虚拟服务器 (端口转发)

DMZ

启用 DMZ 功能	○启用 ⊙禁用
DMZ IP 地址 候选	0 . 0 . 0 . 0

应用

端口 转发 表

应用	协议	外部 IP	外部 端口	内部 IP	内部 端口		
FTP	TCP	*.*.*.* (WAN1)	20 ~ 21	192.168.1.100	20 ~ 21	编辑	删除

创建

出现删除界面。

虚拟服务器 (端口 转发)

删除 转发 策略

应用	FTP
协议	TCP
外部 端口	20~21
重定向 端口	20~21
外部 IP 地址	*.*.*.* (WAN1)
内部 IP 地址	192.168.1.100

Delete

2. 点击 Delete 可以移除虚拟服务器条目。

配置高级设置

高级设置可以让您配置静态路由，动态 DNS，设备管理，IGMP，VLAN 桥接和计划。

配置静态路由

点击**静态路由**打开静态路由列表。

FIGURE 48　　静态路由列表界面

静态路由

静态路由 表

编号	启用	目的地	网络掩码	网关/接口		

创建

创建静态路由条目

点击**创建**增加一个静态路由条目。

FIGURE 49　　创建静态路由条目界面

静态路由

创建策略

策略	○ 启用 ⊙ 禁用		
目的地	0 . 0 . 0 . 0		
网络掩码	0 . 0 . 0 . 0		
网关	0 . 0 . 0 . 0	接口	LAN
花费	0		

应用

策略	选择**启用**可以启用该策略。
目的地	输入静态路由的目标地址段。
网络掩码	输入与地址段相适应的子网掩码。
网关	输入转发到目的网络的网关。
接口	从下拉选项中选择转发的接口。
花费	选择路由的成本。

点击**应用**保存设定。

编辑静态路由条目

参考以下步骤编辑静态路由条目：

1. 在静态路由列表中，点击**编辑**。



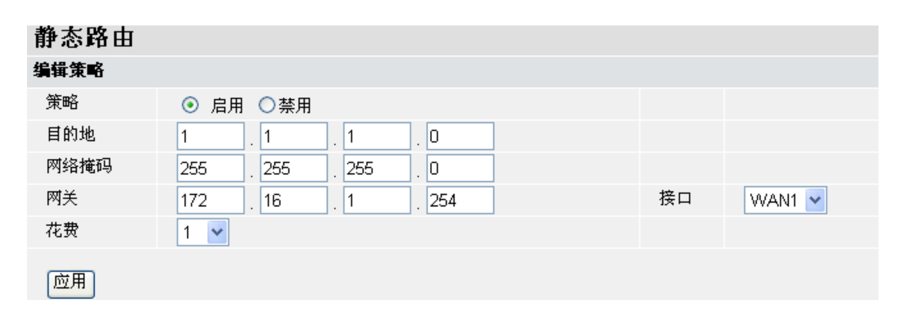
静态路由

静态路由 表

编号	启用	目的地	网络掩码	网关/接口		
1	✓	1.1.1.0	255.255.255.0	172.16.1.254/ WAN1	编辑	删除

创建

以下界面显示了静态路由条目的属性。



2. 编辑静态路由参数。
3. 点击**应用**保存设定。

删除静态路由条目

参考以下步骤删除静态路由条目：

1. 在静态路由列表中，点击**删除**。



出现删除界面。



2. 点击**删除**可以移除静态路由条目。

配置动态 DNS

动态域名管理系统 （DDNS）能够给主机的动态 IP 地址映射一个静态的 DNS 名。如果您的 ISP 没有分配给你静态的 IP 地址，您就可以使用 DNS 名 （例如，billionrouter.dyndns.org）。DNS 名和 IP 地址之间是一对多的映射关系，每一个 DNS 名可以映射多个动态 IP 地址，但是每个 IP 地址只能映射一个 DNS 名。如果用户使用 ADSL PPPoE 和 Cable DHCP 客户端设定他们自己的服务器，例如 Web，Mail，FTP 等服务器。这些 IP 地址都是不固定的，他们将需要 DDNS 获取 IP 地址，用以连接到 Web 服务器，即使 IP 地址不断在变更。

动态 IP 地址是 WAN 接口的 IP 地址。使用 Billion 路由器的 DDNS 功能，首先要在 DDNS 提供商注册帐户，例如 http://www.dyndns.org，然后输入相关的参数，例如注册的域名等。这些都完成了以后，您就会发现只要输入 DNS 名，其就会被解析为 Billion 路由器的 WAN 接口的动态 IP 地址 （可能是 WAN1 接口或 WAN2 接口）。在路由器中，静态域名和动态 IP 地址相对应，IP 地址与 WAN1 接口或 WAN2 接口相关，这些都可以由管理员事先配置。与此同时，一个 WAN 接口可以映射到多个 DNS 名 （例如，billion.dyndns.org 和 billion.billionddns.cn 都可以和 WAN1 接口映射）。

1. 在菜单栏中点击**配置 → 高级 → 动态 DNS** 可以查看动态 DNS 列表。

FIGURE 50 动态 DNS 界面





WARNING: 在使用 DDNS 之前，您需要注册并且拥有由 DDNS 提供商提供的帐户。BiGuard R1000 提供了一些定义的 DDNS 提供商。

2. 点击注册可以注册 Billion 客户共享 DDNS 服务 （2009 年 2 月正式启用）。

3. 在弹出 DDNS **服务注册**页面，在各栏中填入相应的信息，点击**申请**。



DDNS 服务注册

用户基本信息	已注册过用户
用户名：*	（必填）测试用户名是否可用
密码：*	（必填 6-40位字母、数字以及下划线组合）
再次输入密码：*	（必填 6-40位字母、数字以及下划线组合）
请填写有效的邮箱帐号，方便您取回密码!	
电子邮箱：*	（必填）
公司名称：*	（必填）
手机号码：*	（手机或电话至少填一项）
电话号码：*	（电话或手机至少填一项）
QQ帐号：	
MSN用户名：	
SKYPE用户名：	
产品注册信息	
产品型号：*	------请 选 择------ （必填）
产品序列号：*	（必填）序列号是什么??
购买日期：*	- - （必填）
购买地区：*	省份 城市 （必填）
经销商：*	（必填）
申请 重设	

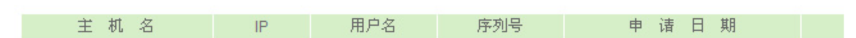
海内存知己 天涯皆BILLION
给您最安心的VPN网络

4. 确认相关信息，若要修改点击**取消**返回上一页面，反之点击**确定**。



5. 点击申请动态域名。


BILLION
BILLION 动态域名服务网
Billion Dynamic DNS Services
登出
Hi, Test1，您好！欢迎使用Billion Dynamic DNS服务！
用 户 信 息
用户名称 Test1 修改密码
电子信箱 tes1@billion.com
公司名称 Billion
手机 138
电话
修改用户信息
您已注册设备资料
序列号 型号 注册日期
G4 BiGuard 2009-04-22 16:52:10 申请动态域名


您已申请的动态域名
主机名 IP 用户名 序列号 申请日期
海内存知己 天涯皆BILLION
给您最安心的VPN网络

6. 填入相关信息，点击**申请**。



7. 恭喜您，动态域名申请成功！



8. 点击**编辑**打开动态域名管理系统的设置界面。

动态 DNS 设置

参数	
动态 DNS	○启用 ⊙禁用
动态 DNS 服务器	NONE
通配符	○启用 ⊙禁用
域名	
用户名	
密码	

应用

动态 DNS	选择**启用**或**禁用**动态 DNS 功能。
动态 DNS 服务器	从下拉选项中选择预定义的 DDNS 服务器。例如，选择 www.dyndns.org(custom)。

通配符	勾选**启用**可以允许 DDNS 通配符。 通配符可以使您注册的那一级域名以下的所有访问都发送到您的设备。例如 *.yourdomain.com。
域名	输入在 DDNS 服务器上注册的 DNS 名。
用户名	输入在 DDNS 服务器上注册的用户名，用于更新注册的 DNS 名和相应的 IP 地址。
密码	输入在 DDNS 服务器上注册的帐户密码，用于更新注册的 DNS 名和相应的 IP 地址。

9. 点击**应用**保存设定。

配置设备管理参数

点击**设备管理**可以更改设备管理参数。

FIGURE 51 设备管理界面



设备名称	
名称	输入设备的名称以和网络中其他设备相区别。
Web 服务器设置	
HTTP 端口	BiGuard R1000 允许用户更改默认的 HTTP 端口。更改众所周知的端口号可以轻易阻止黑客或者 Internet 机器人程序的访问。
IP 地址管理	可以指定管理端的地址，如果保持默认，所有地址的主机都可以管理该设备。
超时自动注销	超过指定的时间不做任何操作，系统就会自动注销。

SNMP 访问控制	
SNMP 功能	可以**启动**或**关闭** SNMP 功能。
SNMP V1 并且 V2	
读社区	输入读社区的名称和 IP 地址。
写社区	输入写社区的名称和 IP 地址。
陷阱社区	输入陷阱社区的名称和 IP 地址。
SNMP V3	
用户名和密码	访问 SNMP 服务器的用户名和密码。
访问权限	可以选择**读**让 SNMP 服务器有只读权限，或者选择**读写**让 SNMP 服务器可读可写。

点击**应用**保存设定。

配置 IGMP

点击 IGMP 可以启用网络二层组播协议。

FIGURE 52　　IGMP 参数界面



IGMP Snooping	可以**启用**或**禁用** IGMP Snooping 功能。
IGMP 代理	可以**启用**或**禁用** IGMP 代理功能。

点击**应用**保存设定。

配置 VLAN 网桥

点击 VLAN Bridge 可以启用 VLAN 网桥。

FIGURE 53　　VLAN 网桥参数界面

VLAN 网桥
VLAN 模式
VLAN 模式
禁用
网桥模式
标注方式
应用

<u>网桥模式</u>

1. 在 VLAN 网桥参数界面中，选择**网桥模式**。

FIGURE 54　　VLAN 网桥模式界面

VLAN 网桥

VLAN 模式

VLAN 模式	○禁用 ◉网桥模式 ○标注方式

应用

VLAN 网桥 表

名称	VLAN ID	标记端口	未标记端口	编辑	删除
Default	1		P1,P2,P3,P4,P5,P6,P7,P8	编辑	

创建

2. 点击**编辑**可以对默认 VLAN 网桥进行编辑。

Edit VLAN

参数

VLAN 名称	Default	VLAN ID	1 (1~4000)
标记的成员端口	☐P1 ☐P2 ☐P3 ☐P4 ☐P5 ☐P6 ☐P7 ☐P8		
未标记的成员端口	☑P1 ☑P2 ☑P3 ☑P4 ☑P5 ☑P6 ☑P7 ☑P8		

应用 取消 返回

3. 一个接口只能属于一个 VLAN，默认情况下所有接口都在 VLAN1 中。如果想创建其他的 VLAN，必须先把 VLAN1 中的相关接口移除。只需不勾选 P1-P8 接口就可以使其从 VLAN1 中移除。例如移除 P1-P4 接口，点击**应用**保存设定。

VLAN 网桥

VLAN 模式

VLAN 模式	○禁用 ◉网桥模式 ○标注方式

应用

VLAN 网桥 表

名称	VLAN ID	标记端口	未标记端口	编辑	删除
Default	1		P5,P6,P7,P8	编辑	

创建

4. 点击**创建**可以创建新的 VLAN 网桥。标记的端口用于交换机之间的连接，未标记的端口用于连接主机。这样的设定使得 WAN1，P1-P4 这 5 个接口都在 WAN1 的子网里面，新增的 4 个接口可以用于连接公共服务器，以供外部网络的用户访问。

Edit VLAN

参数

VLAN 名称	Marketing	VLAN ID	2 (1~4000)
标记的成员端口	☐WAN1 ☐WAN2 ☐P1 ☐P2 ☐P3 ☐P4 ☐P5 ☐P6 ☐P7 ☐P8		
未标记的成员端口	☑WAN1 ☐WAN2 ☑P1 ☑P2 ☑P3 ☑P4 ☐P5 ☐P6 ☐P7 ☐P8		

应用 取消 返回

5. 点击**应用**保存设定。



标注方式

1. 在 VLAN 网桥参数界面中，选择**标注方式**。



2. 输入相应的**标签值**就可以和对端交换机进行通讯。
3. 点击**应用**保存设定。

配置计划

点击**计划**出现时间计划表界面。

FIGURE 55 时间管制界面



时间计划与相应的策略配合可以让管理员或用户在规定的时间内可以使用或不可以使用某一功能或应用。

创建时间计划表

1. 点击**计划**出现时间计划表界面。

FIGURE 56　创建时间管制网络对象

计划

计划 表

名称	一星期中哪天	时间		
**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00		

创建

2. 点击**创建**去创建一个新的时间计划表。

计划

创建

名称	
哪天	☑Sun. ☑Mon. ☑Tue. ☑Wed. ☑Thu. ☑Fri. ☑Sat.
开始时间	08 : 00
结束时间	18 : 00

应用　取消

名称	输入时间管制网络对象的名称。
哪天	输入一个星期中的某些天作为时间管制的时间。
开始时间	从下拉选项中选择开始时间。
结束时间	从下拉选项中选择结束时间。

3. 点击**应用**保存设定。

编辑时间计划表

参考以下步骤编辑时间计划表：

1. 在**时间计划表**界面中，点击**编辑**。

FIGURE 57　编辑时间计划表界面



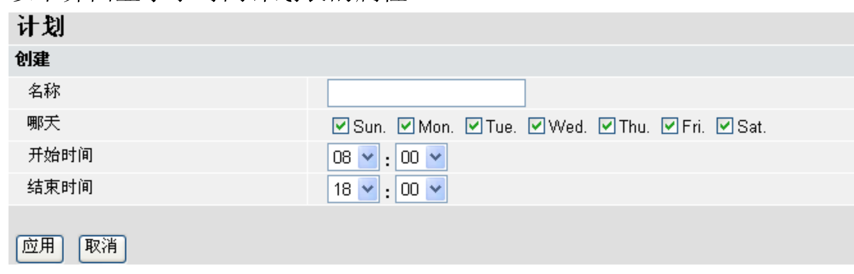
计划

计划 表

名称	一星期中哪天	时间		
**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00		
Workday	Mon. Tue. Wed. Thu. Fri.	From 09:00 To 18:00	Edit	Delete

创建

以下界面显示了时间计划表的属性。



计划

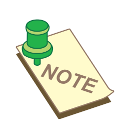
创建

名称	
哪天	☑Sun. ☑Mon. ☑Tue. ☑Wed. ☑Thu. ☑Fri. ☑Sat.
开始时间	08 : 00
结束时间	18 : 00

应用　取消

2. 更改时间计划参数。

3. 点击**应用**保存设定。



NOTE: *在编辑时间计划的时候要格外小心。因为您可能也改变了与此相关的策略。*

删除时间计划表

参考以下步骤删除时间计划表：

1. 在**时间计划表**界面中，点击**删除**。

FIGURE 58 删除时间计划表界面

计划

计划 表

名称	一星期中哪天	时间		
**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00		
Workday	Mon. Tue. Wed. Thu. Fri.	From 09:00 To 18:00	Edit	Delete

创建

出现删除界面。

计划

创建

名称	Workday
哪天	Sun. ☑Mon. ☑Tue. ☑Wed. ☑Thu. ☑Fri. Sat.
开始时间	09 : 00
结束时间	18 : 00

删除 取消

2. 点击**删除**可以删除时间计划表。

配置流量监控系统

点击**流量监控系统**出现流量监控系统界面。

FIGURE 59 流量监控系统界面

流量监控系统

参数

流量监控系统	○启用 ⊙禁用
服务器IP	
Port	8080
Send Period	5 Minutes(5<=Period<1440)

Apply Cancel

流量监控系统用于提供设备的监测统计、流量图显示、用户行为管理以及 Syslog 检测管理功能。

流量监控系统	可以**启用**或**禁用**流量监控系统功能。
服务器 IP	输入服务器 IP 地址。

Port	输入端口号。
Send Period	输入发送时间间隔。

点击 Apply 保存设定。

内容安全管理

BiGuard R1000 可以有效地对网络进行内容安全管理，其主要包括 IM 过滤功能，P2P 过滤功能，游戏过滤功能，股票过滤功能和视频过滤功能。大多数流行的 IM，P2P，游戏，股票和视频软件都可以被过滤。与此同时，通过在路由器里进行不同分组内容安全管理设置，以允许一部分人使用 IM、P2P、股票或视频软件 （如老板、管理层）、而有的电脑是不能使用 IM、P2P、股票或视频软件 （如财务部门、研发技术部门），对提高企业网络信息化办公效率起到了辅助效果。

在**菜单栏**中点击**内容安全管理**就可以进入内容安全管理界面。

FIGURE 60　　内容安全管理界面



3.　点击**创建**就可以创建一个新的组

创建一个组

配置

组过滤	○启用 ⊙禁用
组名	
开始IP地址	
结束IP地址	增加
IP列表	删除
IM过滤列表	□全选 □QQ □MSN □SKYPE □雅虎通 □ICQ □新浪UC □网易泡泡 □阿里旺旺
P2P过滤列表	□严格限制 5 分钟 □全选 □迅雷 □BT □电骡/电驴 □快车 □酷狗 □QQ旋风
游戏过滤列表	□全选 □魔兽世界 □泡泡堂 □梦幻西游 □跑跑卡丁车 □新浪Utgames □中国游戏中心 □QQ游戏 □MSN游戏 □ICQ游戏 □热血江湖 □劲舞团 □街头篮球 □联众 □浩方
股票过滤列表	□全选 □国泰 □操盘手 □大智慧 □钱龙证券 □通达信 □同花顺 □证券之星 □指南针
视频过滤列表	□全选 □PPLive □PPS网络电视 □QQ直播 □悠视网络电视 □迅雷看看 □土豆 □优酷 □Youtube □其他视频
计划 候选	**Always

应用　重置

组过滤	可以选择启用或禁用组过滤功能。
组名	输入您想命名这个组的名称。

开始 IP 地址	输入组中需要过滤的开始 IP 地址。
结束 IP 地址	输入组中需要过滤的结束 IP 地址。
增加	点击增加，开始 IP 地址到结束 IP 地址中的 IP 地址将增加到组中。
IP 列表	显示您需要过滤的 IP 地址
删除	可以删除 IP 地址列表中的 IP 地址
IM 过滤列表	可以勾选或全选需要过滤的 IM 软件，可以选择 **QQ**，**MSN**，**SKYPE**，**雅虎通**，**ICQ**，**新浪 UC**，**网易泡泡**和**阿里旺旺**。
P2P 过滤列表	可以勾选或全选需要过滤的 P2P 软件，可以选择**迅雷**，**BT**，**电骡 / 电驴**，**快车**，**酷狗**和 **QQ 旋风**。 勾选严格限制，可以设定限制的时长。
游戏过滤列表	可以勾选或全选需要过滤的游戏软件，可以选择**魔兽世界**，**泡泡堂**，**梦幻西游**，**QQ 游戏**等网络游戏。
股票过滤列表	可以勾选或全选需要过滤的股票软件，可以选择**国泰**，**操盘手**，**大智慧**，**钱龙证券**，**通达信**，**同花顺**，**证券之星**，**指南针**。
视频过滤软件	可以勾选或全选需要过滤的视频软件，可以选择 PPLive，**PPS 网络电视**，**QQ 直播**，**悠视网络电视**，**迅雷看看**，**土豆**，**优酷**，Youtube 或者**其他视频**。
计划	点击**候选**选择执行 P2P 过滤的时间。这需要事先在**计划**中进行相应的时间计划的设定。

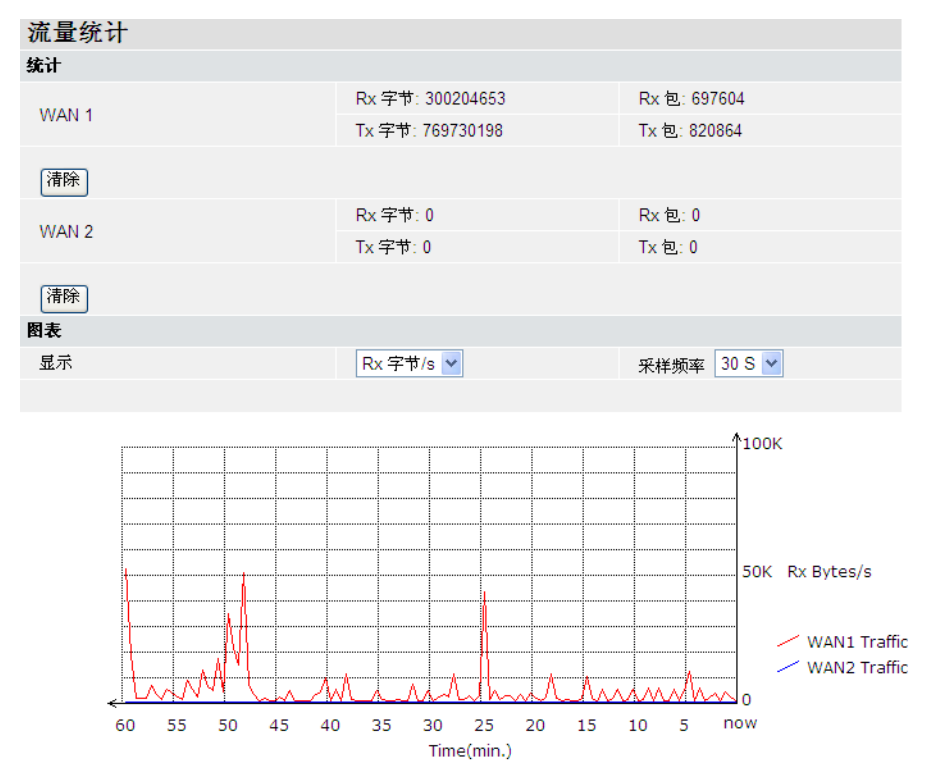
4. 点击**应用**保存设定，点击**重置**重新设置以上各项。

网络安全管理

BiGuard R1000 的网络安全管理功能非常强大，包括了 WAN 流量统计，LAN 流量统计，会话配置，QoS 和防火墙功能。其防火墙功能包含了包过滤，URL 过滤，LAN MAC 过滤，阻塞 WAN 请求和入侵侦测。利用这些安全功能，管理员可以设定适当的策略保护网络，防止非授权的访问和黑客攻击，增强网络的可靠性和安全性。

WAN 流量统计

在**菜单栏**中点击**网络安全管理** →**WAN 流量统计**打开 WAN 流量统计界面。



统计	
WAN1	显示了 WAN1 接口的数据流量统计。 Rx 字节：以字节为单位显示的入站数据流量。 Tx 字节：以字节为单位显示的出站数据流量。 Rx 包：以数据包为单位显示的入站数据流量。 Tx 包：以数据包为单位显示的出站数据流量。 点击**清除**可以清除统计信息。
WAN2	显示了 WAN2 接口的数据流量统计。 Rx 字节：以字节为单位显示的入站数据流量。 Tx 字节：以字节为单位显示的出站数据流量。 Rx 包：以数据包为单位显示的入站数据流量。 Tx 包：以数据包为单位显示的出站数据流量。 点击**清除**可以清除统计信息。

图表	在**显示**字段选择显示的数据流量类型，可选择 Rx 字节 /s，Rx 包 /s，Tx 字节 /s，Tx 包 /s。 在**采样频率**中选择数据采样的周期，可以选择 30S 或 60S。

LAN 流量统计

在**菜单栏**中点击**网络安全管理 →LAN 流量统计**打开 LAN 流量统计界面。

LAN流量统计		
快速设置		
连接限制	连接限制	
过滤规则	Qos	
IP阻塞	包过滤	
LAN流量统计(单击表头排序)	对内IP流量	刷新
IP地址	字节/秒	%
192.168.1.1	743	100
TOTAL 1 User		

快速设置	
连接限制	当用户在 LAN 流量统计中发现问题时可以点击**连接限制**进行策略调整。请参考 连接限制 在 72 页。
过滤规则	当用户在 LAN 流量统计中发现问题时可以点击 QoS 进行策略调整。请参考 配置服务质量参数 在 73 页。
IP 阻塞	当用户在 LAN 流量统计中发现问题时可以点击**包过滤**进行策略调整。请参考 启用包过滤 在 78 页。
LAN 流量统计	
IP 地址	内部主机的 IP 地址。
字节 / 秒	数据流量的大小。
%	显示每个连接的数据流量的百分比。

会话配置

会话配置功能可以让管理员查看连接表，限制会话连接，可以在一定程度上防止 DoS 攻击。

连接表

连接表显示了当前出入站数据流的连接列表，包含会话的协议类型，源 IP，源端口，目的 IP 和目的端口，每页可以显示 10 条会话。

在中点击**连接表**打开连接表界面。

FIGURE 61　　连接表界面

连接 表

连接 表

编号	协议	源IP	源端口	目的IP	目的端口
1	UDP	192.168.1.1	11016	218.64.170.103	8000
2	UDP	192.168.1.1	10000	59.63.131.87	10000
3	UDP	192.168.1.1	10000	117.88.188.254	10000
4	UDP	192.168.1.1	10000	121.33.69.237	10000
5	TCP	192.168.1.254	1060	192.168.1.254	80
6	UDP	192.168.1.1	10000	122.236.102.124	10000
7	UDP	192.168.1.1	10000	125.106.71.100	10000
8	UDP	192.168.1.1	10000	123.149.130.39	10000
9	UDP	192.168.1.1	1809	220.136.32.77	41148
10	UDP	192.168.1.1	4009	119.147.13.226	8000

连接 1 - 10 of 23, 1/3.

过滤　源IP　源端口　目的IP　目的端口

第一　前一个　下一个　最后　**跳到连接**　跳转

编号	显示连接的编号。
协议	显示连接使用的协议。
源 IP	显示连接的源 IP 地址。
源端口	显示连接的源端口号。
目的 IP	显示连接的目标网络 IP 地址。
目的端口	显示连接的目标端口号。
其他按钮	**过滤**：点击**过滤**对显示连接进行筛选。 **源 IP**：输入连接的源 IP 地址。 **源端口**：输入连接的源端口号。 **目的 IP**：输入连接的目标网络 IP 地址。 **目的端口**：输入连接的目标端口号。 **第一**：翻到第一页。 **前一个**：翻到前一页。 **后一个**：翻到后一页。 **最后**：翻到最后一页。 **跳转连接**：输入连接的编号然后按下**跳转**按钮定位到指定连接。

连接限制

连接限制功能可以限制一定的连接数量，以保证网络的正常运行。

在中点击**连接限制**打开连接表界面。

FIGURE 62 连接限制界面

连接限制	
配置	
连接限制	◉ 无限制 ○ 限制每个IP连接最大到 200 ☐ 高级配置 ◉ 拒绝来自这个IP新的连接 5 分钟. ○ 丢弃来自这个IP的所有包 5 分钟.
应用	

无限制	对网络连接没有任何限制。
限制每个 IP 连接最大到	输入每个 IP 最大的连接数量。如果超过这个数值，该 IP 地址将不能够建立新的连接。
高级配置	勾选这个选项可以进行高级配置。 • **拒绝来自这个 IP 新的连接**：如果选择这个选项，那么在一定时间内，如 5 分钟内，设备将拒绝该 IP 地址的所有新连接。 • **丢弃来自这个 IP 的所有包**：如果选择这个选项，那么在一定时间内，如 5 分钟内，设备将丢弃该 IP 地址的所有数据包。

点击**应用**保存设定。

配置服务质量参数

服务质量指的是定义的数据通讯系统的性能级别，用于应用到指定的数据流上。例如实时语音视频需要一个保证带宽才能正常工作，服务质量保证了这样的带宽。另外，服务质量还可以应用优先级。

1. 点击 QoS 可以查看和配置服务质量参数。

FIGURE 63 服务质量界面

服务质量		
WAN 1 出站		
QoS功能	○启用 ◉禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
WAN 1 入站		
QoS功能	○启用 ◉禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
WAN 2 出站		
QoS功能	○启用 ◉禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
WAN 2 入站		
QoS功能	○启用 ◉禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
应用		

创建服务质量规则

1. 在服务质量界面点击**规则表**进入服务质量规则界面。

服务质量					
WAN1出站 QoS 规则表 (总共 0 规则 使用 / 最大 150 规则.)					
应用	保证	最大	优先级		
未分配的 带宽		102400 kbps (100%)			
创建					

2. 点击**创建**，进入 QoS **策略**界面，然后输入相关参数。

FIGURE 64　　创建服务质量规则界面

服务质量		
增加 QoS 策略		
接口	WAN1出站	
应用		
保证	1 kbps	
最大	102400 kbps	
优先级	3 (普通)	
DSCP 标记	黄金服务(L)	
地址 类型	⦿IP 地址 ○MAC 地址	
带宽 类型	⦿ 共享带宽 ○所有源IP地址平分带宽	
源 IP 地址 范围	从 0.0.0.0	到 255.255.255.255
目的地 IP 地址 范围	从 0.0.0.0	到 255.255.255.255
协议	任何	
源 端口 范围 助手	从 1	到 65535
目的地 端口 范围 助手	从 1	到 65535
DSCP	Any	
计划 候选	**Always	
应用		

接口	根据接口的不同可以有 WAN1 出站，WAN1 入站，WAN2 出站，WAN2 入站。
应用	输入 QoS 策略的名称。
保证	输入一个数值保证最小的带宽。
最大	输入一个数值限定最大的带宽。
优先级	选择 QoS 的优先级。0 是最低，6 是最高，默认是 3。
DSCP 标记	DSCP 标记，也是众所周知的 Diff-Serv，可以基于 IP 的 DSCP 数值分类数据流。它根据每个报文指定的 QoS 来提供特定的服务，可以用不同的方法来指定报文的 QoS，如 IP 报文优先，报文的源和目的地址等，网络通过这些信息来进行报文的分类、流量整形、流量监管和队列调度。 可以选择**尽力传送，保证，黄金服务，白银服务和青铜服务**。
地址类型	可以选择 QoS 策略应用的地址类型，可以选择 **IP 地址**或 **MAC 地址**。
带宽类型	选择让所有的源 IP 地址共享带宽还是平分带宽。
源 IP 地址范围	输入 QoS 策略应用的源 IP 地址范围。如果选择地址类型是 **MAC 地址**，该字段就成为**源 MAC 地址**。
目的地 IP 地址范围	输入 QoS 策略应用的目的 IP 地址范围。如果选择地址类型是 **MAC 地址**，该字段就不存在。

协议	可以选择数据流使用的协议，可以选择**任何**，TCP，UDP 和 ICMP。
源端口范围	输入 QoS 策略应用的源端口范围。可以点击**助手**选择预定义的应用端口。
目的地端口范围	输入 QoS 策略应用的目的端口范围。可以点击**助手**选择预定义的应用端口。
DSCP	
计划	点击**候选**选择计划时间。

3. 点击**应用**保存设定。



编辑服务质量规则

参考以下步骤编辑 QoS 规则：

1. 在服务质量界面规则中，点击**编辑**。

FIGURE 65 编辑服务质量规则界面



以下界面显示了服务质量规则的属性。



2. 编辑服务质量参数。

3. 点击**应用**保存设定。

删除服务质量规则

参考以下步骤删除服务质量规则：

1. 在服务质量规则界面中，点击**删除**。

FIGURE 66　删除服务质量规则界面

服务质量					
WAN1出站 QoS 规则表（总共 2 规则 使用 / 最大 150 规则.）					
应用	保证	最大	优先级		
Busy	1024 kbps	2048 kbps	3	编辑	删除
未分配的 带宽		101376 kbps (99%)			
创建					

出现删除界面。

服务质量		
删除 QoS 策略		
接口	WAN1出站	
应用	Busy	
保证	1024	
最大	2048kbps	
优先级	3kbps	
DSCP 标记	黄金服务（低）	
地址 类型	IP 地址	
源 IP 地址 范围	From 192.168.1.1	To 192.168.1.100
目的地 IP 地址 范围	From 1.1.1.1	To 1.1.1.100
协议	任何	
源 端口 范围	From 0	To 0
目的地 端口 范围	From 0	To 0
DSCP	Any	
计划	**Always	
删除		

2. 点击**删除**移除服务质量规则。

配置 SIP 服务质量

SIP （会话初始协议）是由 IETF （Internet 工程任务组织）开发的信令控制协议。SIP 是一种整合了 Internet 和 PSTN 环境的技术。它和 HTTP 协议比较相似，都基于文本编码发送命令和消息，以确保协议简单化并由文本所确定而不是信号。SIP 正如其名，就是会话的初始协议，与其他协议一起工作。SIP 使用 SDP （会话描述协议，RFC2327，RFC2365）来描述会话的消息内容。SIP 的会话仅仅是 RTP （实时传输协议）的数据流，它可以承载实时数据，语音或视频。

这儿有不同的 SIP 功能和组件。SIP 组件包括：用户代理 （UA），是终端用户设备，如用于创建和管理 SIP 会话的移动电话、多媒体手持设备、PC、PDA 等。用户代理服务器对消息进行响应。代理服务器，接受 SIP UA 的会话请求并查询 SIP 注册服务器，获取收件方 UA 的地址信息。然后，它将会话邀请信息直接转发给收件方 UA （如果它位于同一域中）或代理服务器 （如果 UA 位于另一域中）。重定向服务器，允许 SIP 代理服务器将 SIP 会话邀请信息定向到外部域。SIP 重定向服务器可以与 SIP 注册服务器和 SIP 代理服务器同在一个硬件上。注册服务器，是包含域中所有用户代理的位置的数据库。在 SIP 通信中，这些服务器会检索参与方的 IP 地址和其他相关信息，并将其发送到 SIP 代理服务器。语音邮件服务器 （语音信箱）等等。

SIP 功能整合了相关的服务，例如 PSTN，H.323，MGCP，MEGECO 等等，甚至大多数 3G 服务都是基于 SIP 协议的。

QoS （服务质量）是一套为数据传输保证质量的机制。QoS 提供了不同的优先级区分不同的用户和数据流，或者为应用保证某一性能级别。如果网络容量不充足，QoS 的保证机制是很重要的，尤其是流媒体应用，例如 VoIP 和 IPTV，因为这些应用往往需要固定的速率并且具有延迟敏感性。

BiGuard R1000 的服务质量 （QoS）可以管理应用的数据流，例如 FTP 和 SMTP。在路由器上增添了数据流控制功能以后，QoS 功能就可以控制和管理 SIP 服务的数据流。管理员可以控制公司外部用户访问企业内部网的带宽或者公司内部人员访问 Internet 的带宽。

请参考以下步骤配置 SIP 服务质量：

1. 点击**网络安全管理 →QoS** 打开服务质量界面。

服务质量		
WAN 1 出站		
QoS功能	○启用 ⊙禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
WAN 1 入站		
QoS功能	○启用 ⊙禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
WAN 2 出站		
QoS功能	○启用 ⊙禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
WAN 2 入站		
QoS功能	○启用 ⊙禁用	规则表
最大ISP带宽	102400 kbps	带宽 设置
应用		

2. 在服务质量界面点击**规则表**进入服务质量规则界面。



3. 点击**创建**，进入 **QoS 策略**界面，然后输入相关参数。



4. 点击**应用**保存设定。



配置防火墙

在**菜单栏**中点击**网络安全管理 → 防火墙**可以设定包过滤，URL 过滤，LAN MAC 过滤，阻塞 WAN 请求，入侵检测和 ALG。

启用包过滤

点击**包过滤**显示包过滤列表：



包过滤可以限制网络上传输的数据类型。

<u>创建包过滤参数</u>

1. 点击**创建**增加一个新的包过滤条目。

FIGURE 67　创建包过滤参数界面

包 过滤

增加 过滤规则

字段	设置
ID	1
策略	启用 / 禁用
匹配时作用	丢弃
方向	出站
源 IP	任何；开始IP地址 0.0.0.0；结束IP地址 0.0.0.0；网络掩码 0.0.0.0
目的地 IP	任何；开始IP地址 0.0.0.0；结束IP地址 0.0.0.0；网络掩码 0.0.0.0
协议	任何
源 端口 范围 助手	1 ~ 65535
目的地 端口 范围 助手	1 ~ 65535
计划 候选	**Always
日志	启用 / 禁用

应用　反向应用

ID	输入包过滤条目的 ID （只能输入 1-999 之间的数值）。
策略	勾选**启用**可以启用该包过滤条目。
匹配时作用	从下拉选项中选择动作应用的指定的数据包： • 丢弃：丢弃数据包。 • 转发：发送数据包。
方向	从下拉选项中选择包的流动方向： • **出站**：过滤从 LAN 接口到 WAN 接口的数据包。 • **入站**：过滤从 WAN 接口到 LAN 接口的数据包。
源 IP	在下拉选项中选择**任何**，**子网**，IP **范围**或**单一地址**，然后在后面的地址和网络掩码字段输入相应的参数。
目的地 IP	在下拉选项中选择**任何**，**子网**，IP **范围**或**单一地址**，然后在后面的地址和网络掩码字段输入相应的参数。
协议	在下拉选项中选择应用包过滤规则数据流量的协议，可以选择**任何**，TCP 或 UDP。
源端口范围	输入应用包过滤规则的数据流量的源端口范围。可以点击**助手**选择预定义的应用端口。
目的地端口范围	输入应用包过滤规则的数据流量的目的端口范围。可以点击**助手**选择预定义的应用端口。
计划	点击**候选**选择计划时间。
日志	勾选**启用**可以在过滤器运行的时候创建一个日志文件。

2. 点击**反向应用**保存设定，这样可以让包过滤规则应用在出站和入站两个方向。或者点击**应用**保存设定。

一旦创建了一个或者多个条目，就可以点击**移动**去移动条目，以此改变策略的优先级。序号越小，执行最优先，优先权最大的是 #1，反之亦然。



包 过滤

包 过滤 表

ID	启用	动作	方向	源IP	目的IP	协议	源端口	目的端口			
1	✓	丢弃	出站	任何	任何	所有	任何	任何	编辑	删除	移动
2	✓	丢弃	出站	任何	任何	所有	任何	任何	编辑	删除	移动

创建

编辑包过滤参数

参考以下步骤编辑包过滤条目：

1. 在包过滤参数界面中，点击**编辑**。

FIGURE 68 编辑包过滤参数界面

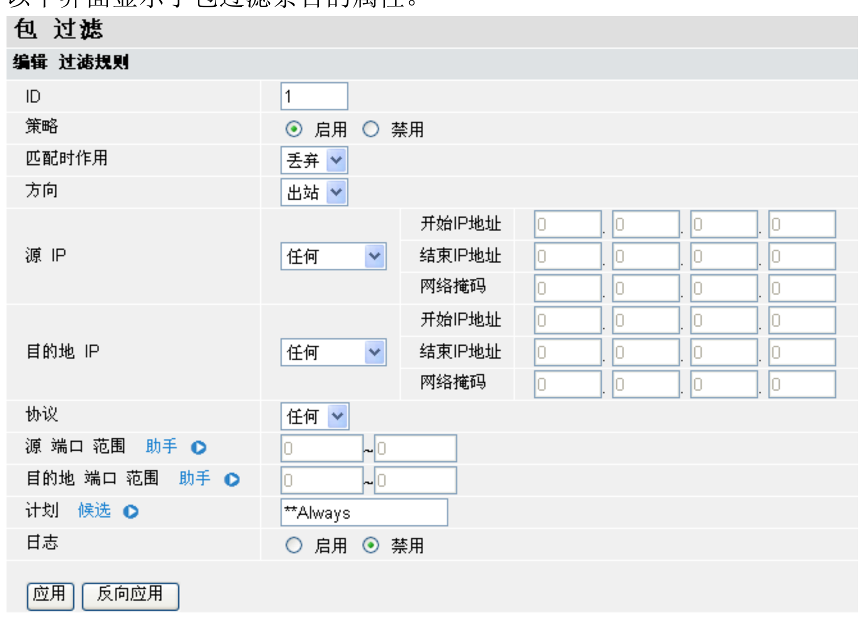
包 过滤

包 过滤 表

ID	启用	动作	方向	源IP	目的IP	协议	源端口	目的端口			
1	✓	丢弃	出站	任何	任何	所有	任何	任何	编辑	删除	移动

创建

以下界面显示了包过滤条目的属性。



2. 对包过滤参数进行更改。

3. 点击**应用**保存设定。

删除包过滤参数

参考以下步骤删除包过滤条目：

1. 在包过滤参数界面，点击**删除**。

FIGURE 69　　删除包过滤条目界面

包 过滤

包 过滤 表

ID	启用	动作	方向	源IP	目的IP	协议	源端口	目的端口			
1	✓	丢弃	出站	任何	任何	所有	任何	任何	编辑	删除	移动

创建

出现删除界面。

包 过滤

请确认删除下面的过滤规则

ID	1
策略	启用
匹配时作用	丢弃
方向	出站
源 IP	任何
目的地 IP	任何
协议	所有
源 端口 范围	任何
目的地 端口 范围	任何
计划	**Always

删除

2. 点击**删除**移除包过滤参数条目。

配置 URL 过滤

点击 **URL 过滤**可以配置 URL 过滤规则。URL 过滤规则可以启用和关闭关键字过滤，域名过滤和限制 URL 特性网络对象。

FIGURE 70　　配置 URL 过滤规则界面

URL 过滤

配置

URL 过滤	○ 启用　◉ 禁用
关键字 过滤	☐启用　细节
域名过滤	☐启用　细节
	☐禁止访问信任域名以外的域名
限制URL特性	☐阻塞 Java Applet
	☐阻塞 ActiveX
	☐阻塞 Web 代理
	☐阻塞 Cookie
	☐用IP地址阻塞上网
日志	☐启用

应用

例外列表

名称	IP 地址		

创建

创建 URL 过滤规则

1. 在菜单栏中点击**网络安全管理 → 防火墙 →URL 过滤**可以配置 URL 过滤规则。

FIGURE 71　创建 URL 过滤规则界面

URL 过滤

配置

URL 过滤	○ 启用 ◉ 禁用
关键字 过滤	☐ 启用 细节
域名过滤	☐ 启用 细节
	☐ 禁止访问信任域名以外的域名
限制URL特性	☐ 阻塞 Java Applet
	☐ 阻塞 ActiveX
	☐ 阻塞 Web 代理
	☐ 阻塞 Cookie
	☐ 用IP地址阻塞上网
日志	☐ 启用

应用

例外列表

名称	IP 地址		

创建

URL 过滤	选择**启用**或**禁用**该 URL 过滤规则。
关键字过滤	勾选**启动**激活关键字过滤，点击**细节**创建关键字过滤网络对象。
域名过滤	勾选**启动**激活关键字过滤，点击**细节**创建一个域名过滤网络对象。 勾选**禁止访问信任域名以外的域名**就只能访问那些受信的域名。
限制 URL 特性	勾选多个 URL 特性以启用限制 URL 特性过滤，包括**阻塞 Java Applet**，**阻塞 ActiveX**，**阻塞 Web 代理**，**阻塞 Cookie** 和**用 IP 地址阻塞上网**。
日志	勾选**启动**可以为该规则创建一个日志文件。

2. 点击**应用**保存设定。

<u>创建关键字过滤网络对象</u>

1. 在 **URL 过滤**界面中的**关键字过滤**字段点击**细节**。

FIGURE 72　创建 URL 过滤网络对象界面

关键字 过滤

创建

关键字	

应用

当包含这些关键字时阻塞WEB URLs

编号	关键字	
1	sex	删除

2. 在**关键字**字段中输入关键字并点击**应用**增加关键字过滤。

   关键字将被列在**当包含这些关键字时阻塞 WEB URLs**。
3. 点击**删除**可以删除列表中的关键字。
4. 点击**应用**保存设定。

创建域名过滤网络对象

1. 在 URL **过滤**界面中的**域名过滤**字段点击**细节**。

FIGURE 73 创建域名过滤网络对象界面

域名过滤
创建
域名
类型 禁止 域名
应用
信任 域名 表
编号 域名
禁止 域名 表
编号 域名

域名	输入禁止或信任的域名。
类型	选择域名类型： • 禁止域名：用户将被阻止访问这些域名。选择这个选项点击**应用**就可以添加到**禁止域名表**中。 • 信任域名：用户将被允许访问这些域名。选择这个选项点击**应用**就可以添加到**信任域名表**中。

2. 点击**应用**保存设定。

创建 URL 过滤例外列表

1. 在 URL **过滤**界面中的点击**创建**进入创建例外列表的界面，该列表中的 IP 地址不受 URL 过滤规则影响。

FIGURE 74 创建 URL 过滤例外界面

例外
创建
名称
IP 地址 候选 0 . 0 . 0 . 0
应用

名称	URL 过滤例外列表的名称。
IP 地址	输入例外的 IP 地址，也可以点击**候选**选择一个现有的 IP 地址。

2. 点击**应用**保存设定。

配置 LAN MAC 地址过滤

LAN MAC 地址过滤可以阻止指定 LAN MAC 地址的访问。

FIGURE 75　LAN MAC 地址过滤界面

Ethernet MAC 过滤

缺省 策略

动作　转发　丢弃

应用

策略 列表

编号	启用	动作	MAC 地址	IP 地址

创建

创建 LAN MAC 地址过滤，首先点击 **LAN MAC 过滤**。

在缺省策略中选择**转发**或**丢弃**，可以决定 LAN MAC 过滤规则在默认情况下的动作。

创建 LAN MAC 地址过滤

1. 点击**创建**增加一条 LAN MAC 地址过滤规则。

FIGURE 76　创建以 LAN MAC 地址过滤界面

Ethernet MAC 过滤

创建规则

策略　启用　禁用

匹配时作用　丢弃

Mac 地址　候选

绑定 IP　启用　禁用

IP 地址

日志　启用　禁用

应用

策略	勾选**启用**可以启用该 LAN MAC 地址过滤规则。
匹配时作用	从下拉选项中选择动作： • 丢弃：丢弃该数据包。 • 转发：发送该数据包。
MAC 地址	如果想过滤的 MAC 地址或者点击**候选**查看可用的 MAC 地址，然后从中选择一个。
绑定 IP	可以**启用**或者**禁用**绑定 IP 地址到指定的 MAC 地址。也就是说过滤策略不仅仅要判断 MAC 地址，还需要判断 IP 地址，只有两者都符合条件才可以进行相应的动作。
IP 地址	输入绑定 IP 的地址。
日志	勾选**启动**可以为该规则创建一个日志文件。

2. 点击**应用**保存设定。

编辑 LAN MAC 地址过滤规则

参考以下步骤编辑 LAN MAC 地址过滤规则：

1. 在 LAN MAC 地址过滤界面中，点击**编辑**。

FIGURE 77　　编辑 LAN MAC 地址过滤界面

Ethernet MAC 过滤

缺省 策略

动作　◉ 转发 ○ 丢弃

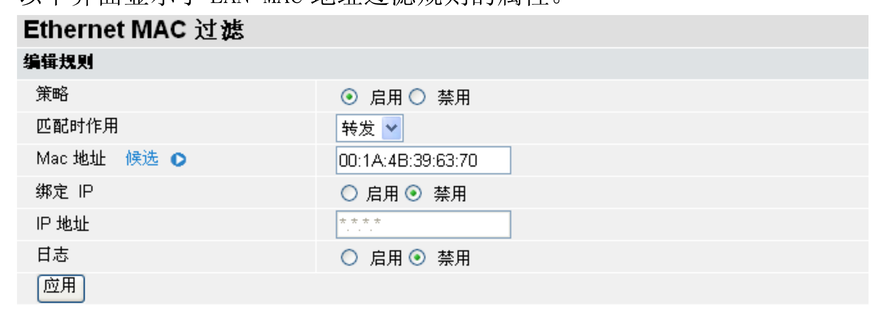
[应用]

策略 列表

编号	启用	动作	MAC 地址	IP 地址		
1	✓	转发	00:1A:4B:39:63:70	*.*.*.*	编辑	删除

创建

以下界面显示了 LAN MAC 地址过滤规则的属性。



2. 更改 LAN MAC 地址过滤规则的参数。
3. 点击**应用**保存设定。

删除 LAN MAC 地址过滤规则

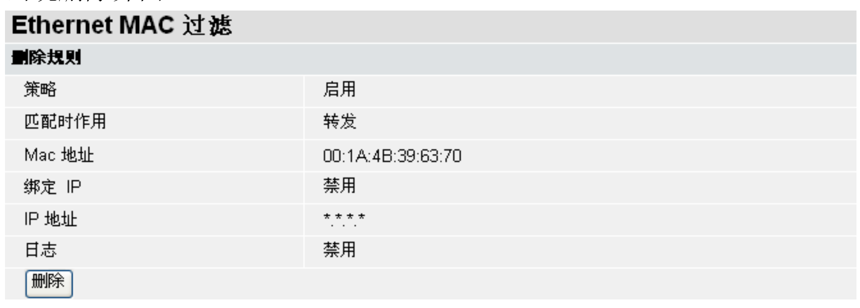
参考以下步骤删除 LAN MAC 地址过滤规则：

1. 在 LAN MAC 地址过滤参数界面，点击**删除**。

FIGURE 78　　删除 LAN MAC 地址过滤规则



出现删除界面。



2. 点击**删除**可以删除 LAN MAC 地址过滤规则。

阻塞 WAN 请求

在菜单栏中点击**网络安全管理 → 防火墙 → 阻塞 WAN 请求**可以配置阻塞 WAN 请求。

FIGURE 79 阻塞 WAN 请求界面

阻塞WAN请求	
启用以阻止来源于Internet，例如骇客的攻击。	
阻塞WAN请求	⦿启用 ○禁用
阻塞WAN ICMP请求	⦿启用 ○禁用
应用	

阻塞 WAN 请求	启用该功能可以阻塞 WAN 接口上的所有数据包的请求。
阻塞 WAN ICMP 请求	启用该功能可以阻塞 WAN 接口上的 ICMP 数据包的请求，也就是无法 Ping 通 WAN 接口。

点击**应用**保存设定。

配置入侵侦测

在菜单栏中点击**网络安全管理 → 防火墙 → 入侵侦测**可以配置入侵侦测。

FIGURE 80 配置入侵侦测界面

入侵侦测	
启用以阻止来自Internet的黑客攻击	
入侵侦测	⦿启用 ○禁用
入侵 日志	○启用 ⦿禁用
入侵侦测功能列表	☐防止WAN1 Land 攻击 ☐SPI 保护 ☐ 防止WAN2 Land 攻击 ☐防止特洛伊木马扫描 ☐防止Back Orifice扫描 ☐防止Netbus扫描 ☐防止SYN/FIN扫描 ☐防止XMAS扫描 ☐防止TCP端口扫描 ☐防止UDP端口环路 ☐防止洪水攻击 ☐拒绝从WAN口连接 ☐所有列表
ARP 保护	○启用 ⦿禁用
应用	

入侵侦测	可以**启用**或**禁用**入侵侦测功能。
入侵日志	可以**启用**或**禁用**入侵侦测的日志功能，以决定是否把入侵事件记录在日志中。

入侵侦测功能列表	勾选相应的入侵侦测功能，以对这些入侵事件进行识别。可以选择： • 防止 WAN1 Land 攻击 • SPI 保护 • 防止 WAN2 Land 攻击 • 防止特洛伊木马扫描 • 防止 Back Orifice 扫描 • 防止 Netbus 扫描 • 防止 SYN/FIN 扫描 • 防止 XMAS 扫描 • 防止 TCP 端口扫描 • 防止 UDP 端口环路 • 防止洪水攻击 • 拒绝从 WAN 口连接 • 所有列表
ARP 保护	可以**启用**或**禁用** ARP 保护功能。

点击**应用**保存设定。

配置应用层网关

在菜单栏中点击**网络安全管理 → 防火墙 →ALG** 可以配置应用层网关。

FIGURE 81 配置应用层网关界面

应用层网关	
应用层网关	
SIP ALG	⦿启用 ○禁用
PPTP ALG	⦿启用 ○禁用
IRC ALG	⦿启用 ○禁用
SNMP ALG	⦿启用 ○禁用
SPPTP ALG	⦿启用 ○禁用
TFTP ALG	⦿启用 ○禁用
AMANDA ALG	⦿启用 ○禁用
FTP ALG	⦿启用 ○禁用
H323 ALG	⦿启用 ○禁用
应用	

SIP ALG	可以**启用**或**禁用** SIP ALG 功能。
PPTP ALG	可以**启用**或**禁用** PPTP ALG 功能。
IRC ALG	可以**启用**或**禁用** IRC ALG 功能。
SNMP ALG	可以**启用**或**禁用** SNMP ALG 功能。
SPPTP ALG	可以**启用**或**禁用** SPPTP ALG 功能。
TFTP ALG	可以**启用**或**禁用** TFTP ALG 功能。
AMANDA ALG	可以**启用**或**禁用** AMANDA ALG 功能。

FTP ALG	可以**启用**或**禁用** FTP ALG 功能。
H323 ALG	可以**启用**或**禁用** H323 ALG 功能。

点击**应用**保存设定。

日志和 E-mail 通知

BiGuard R1000 使用工业标准的警报协议抓取网络活动信息。这些信息被保存成日志的形式，发送到日志服务器或者是选定的 E-mail 地址。

日志配置

1. 点击**日志配置**打开日志配置界面。

FIGURE 82 日志配置界面

日志 配置

参数

目录	系统 日志	系统日志 服务器	E-mail 报警
系统维护	☑	☐	☐
系统错误	☑	☐	☐
访问控制	☐	☐	☐
包过滤	☐	☐	☐
LAN MAC过滤	☐	☐	☐
URL过滤	☐	☐	☐
入侵侦测	☐	☐	☐
调用数据记录	☐	☐	☐
点对点	☐	☐	☐
远程访问	☐	☐	☐
IM	☑	☐	☐
P2P	☑	☐	☐
股票	☑	☐	☐
游戏	☑	☐	☐
视频	☑	☐	☐

应用

目录	勾选**系统日志**抓取日志信息在设备上。 勾选**系统日志服务器**抓取日志并发送到系统日志服务器。 勾选 **E-mail 报警**发送日志到指定的 E-mail 帐户。
系统维护	启用系统维护的日志报告。
系统错误	启用系统或硬件错误消息的日志报告。
访问控制	启用访问控制的日志报告。
包过滤	启用包过滤的日志报告。 **注意：**包过滤不会中断停留在 LAN 端的数据报。
LAN MAC 地址过滤	LAN MAC 地址过滤使得管理员能够控制访问。如果 MAC 地址被阻止了，BiGuard R1000 将不会响应 MAC 地址的任何请求。（例如：如果设备试图访问有病毒的路由器）
URL 过滤	URL 过滤可以防止非授权访问。
入侵侦测	入侵侦测事件的日志。
调用数据记录	勾选这个选项使得调用数据记录的日志被记录下来。
点对点	勾选这个选项使得 PPP 的日志被记录下来。

远程访问	启用远程访问的日志报告。
IM	启用 IM 通讯软件的日志报告。
P2P	启用使用 P2P 下载软件的日志报告。
股票	启用使用股票软件的日志报告。
游戏	启用网络游戏的日志报告。
视频	启用使用视频软件的日志报告。

2. 点击**应用**保存设定。

系统日志服务器

系统日志服务器使得设备能够传送事件和通知消息到使用 syslog 协议的服务器。操作系统在进程的开始或结束发送消息报告进程状态。

FIGURE 83　　系统日志服务器界面

系统日志 服务器
参数
发送日志到远程服务器　启用　禁用
日志 服务器 地址
应用

发送日志到远程服务器	可以选择**启用**或**禁用**发送日志到远程服务器的功能。
日志服务器地址	输入日志服务器的 IP 地址。

点击**应用**保存设定。

E-Mail 报警

这个部分可以让设备发送安全事件日志到指定的 E-Mail 帐户。

FIGURE 84 E-MAIL 报警界面

E-Mail 报警

参数	
E-Mail 报警	○启用 ◉禁用
接收者的 E-Mail 地址	
发送者的 E-Mail 地址	
SMTP 邮件服务器	
邮件服务器 登陆	○启用 ◉禁用
用户名	
密码	••••••
通过电子邮件报警时机	○立即 ○每小时 ○每日 12:00 ◉A.M. ○P.M. ○每周 Sunday ◉当日志已满

应用

E-Mail 报警	使得安全相关的事件日志被发送到指定的 E-Mail 帐户。启动的时候，下面的字段才有效。
接收者的 E-Mail 地址	输入接收日志通知的 E-Mail 地址。
发送者的 E-Mail 地址	输入发送日志通知的 E-Mail 地址。
SMTP 邮件服务器	输入发送日志通知的 SMTP 服务器地址。
邮件服务器登陆	如果需要用户登陆，请**启用**该功能。
用户名	输入接收者的 E-Mail 帐户名。
密码	输入发送者的 E-Mail 地址帐户密码。
通过电子邮件报警时机	可以选择**立即**，**每小时**，**每日时间**，**每周的哪一天**和**当前日志已满**。

点击**应用**保存设定。

保存配置到 Flash 存储器

这个功能可以让您保存当前在内存中的配置到 Flash 存储器中。

FIGURE 85　　保存配置到 FALSH 的界面

保存配置到闪存中

请确认你愿意保存配置。

当配置信息写到闪存芯片中时会有一些延迟。

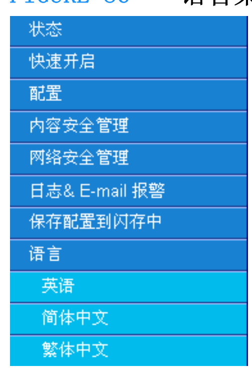
应用

点击**应用**保存配置到 Falsh 存储器。

语言选择

语言选择提供了三种不同的界面显示语言。（包括英文，简体中文和繁体中文）

FIGURE 86　　语言菜单



点击语言名称，然后设备的界面将会变成您选择的语言界面。

故障排错

前言

附录部分介绍了您在安装硬件和配置 BiGuard R1000 时可能出现的问题。在开始排错以前，确保您已经正确安装了硬件。

网络设定

许多家庭有不止一台电脑。这些电脑通过一个集线器，路由器或交换机彼此相联，从而构成一个网络。

所有的电脑（或者像打印机一样的设备）在一个网络中，就必须有各自的 IP 地址。IP 地址可以手工设定（静态 IP 地址），或者可以由 DHCP 路由器或服务器自动分配（动态 IP 地址）。在有线和无线连接中都是一模一样的。

查看 IP 地址的类型

参考以下步骤查看您的电脑是自动获取还是手工设定的 IP 地址。

1. 在 Windows 操作系统中点击**开始** → **运行**。
2. 在运行中输入 cmd，然后点击**确定**。
3. 在命令提示符中输入 ipconfig /all。

   查看 DHCP Enabled 这一行。

```
C:\WINDOWS\system32\cmd.exe
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : localdomain

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-9A-29-40
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.163.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.163.2
        DHCP Server . . . . . . . . . . . : 192.168.163.254
        DNS Servers . . . . . . . . . . . : 192.168.163.2
        Primary WINS Server . . . . . . . : 192.168.163.2
        Lease Obtained. . . . . . . . . . : Thursday, October 16, 2008 4:38:28 P
M
        Lease Expires . . . . . . . . . . : Thursday, October 16, 2008 5:08:28 P
M

C:\Documents and Settings\Administrator>_
```

如果启用了 DHCP，那么您的路由器就会自动分配 IP 地址。您就可以在网络设定中使用动态设定。

如果没有启用 DHCP，那么您必须手工配置 IP 地址。

硬件问题

这部分将解决关于 BiGuard R1000 的硬件问题。

BiGuard R1000 无法启动

如果在您打开 BiGuard R1000 的时候，其电源，状态，WAN，LAN 和 DMZ 的 LED 灯都不亮，请检查以下内容：

- 确保电源线正确连接在设备和电源插座上。

检查您正在使用的 12V DC 电源适配器是否是 Billion 的产品。

如果仍然不可用，您可能遇到了硬件上的问题。请联系技术支持。

BiGuard R1000 的 LED 灯在启动后持续亮着

当 BiGuard R1000 在启动时，LED 灯会亮 10 秒钟然后就不亮了。如果所有的 LED 灯都持续亮着，那就是硬件有问题了。

如果在启动后一分钟所有的 LED 灯都亮着：

- 反复按电源按钮看看是否能够恢复正常。
- 重置配置到出厂默认配置。

如果仍然不可用，您可能遇到了硬件上的问题。请联系技术支持。

BiGuard R1000 的 LAN 或者 WAN 接口的 LED 灯不亮

如果建立以太网连接的时候，LAN 或 WAN 的 LED 灯不亮，你需要检查以下内容：

- 确保每根以太网线都连着防火墙和集线器或工作站。
- 确保连接的集线器或工作站的电源是开着的。
- 确保网线没有问题。当把防火墙的 Internet 接口连接到 Cable 调制解调器或 DSL 调制解调器，使用调制解调器支持的网线。这种网线可以是标准的直通线或者是以太网交叉线。

忘记密码

- 首先尝试输入默认的用户名和密码：
  用户名：admin
  密码：admin



NOTE: *用户名和密码都是大小写敏感的。*

如果这没有用，请按住路由器背面的 Reset 按钮恢复 BiGuard R1000 到出厂默认配置，直到状态 LED 开始闪烁为止。然后输入默认的用户名和密码登录设备。



NOTE: *恢复出厂默认配置将会删除所有先前的配置信息。强烈建议在重置路由器之前先保存配置文件。*

LAN 接口问题

参考以下部分解决 BiGuard R1000LAN 接口的相关问题。

不能从 LAN 端访问 BiGuard R1000

从 LAN 端连接 BiGuard R1000 没有任何响应：

- 检查是否使用了正确的以太网线缆类型并确保网线的两端分别连接了电脑和路由器。
- 确保电脑的以太网适配器已经正确安装并且功能正常。参考电脑的相关文档。

如果仍然不可用，您可能遇到了硬件上的问题。请联系技术支持。

不能 Ping 通 LAN 端的任何电脑

- 检查 BiGuard R1000 前面板的 10/100M LAN 接口 LED 灯。至少一个 LED 灯要亮。如果都不亮，检查 BiGuard R1000 和集线器或者电脑之间的网线连接。
- 确保电脑的以太网适配器相连的那个 LAN 接口的 LED 灯是亮的。
- 确保电脑以太网适配器的驱动软件和 TCP/IP 的软件已经正确安装并配置。
- 确保 BiGuard R1000 的 IP 地址和子网掩码是正确的，并且电脑的与 BiGuard R1000 在同一子网。

日期时间不同步

如果日期和时间不能正确显示，请使用 Web 配置界面配置 BiGuard R1000 的日期和时间。日期和时间的设定在菜单栏中的**配置 → 系统 → 时区**。

若要同步日期和时间，打开 Web 配置界面的**状态**界面，然后点击界面上的**对时**。

不能访问 BiGuard R1000 的 Web 配置界面

从一台连接到网络的电脑无法访问 BiGuard R1000 的 Web 配置界面：

- 检查电脑和路由器之间的连接。
- 确保电脑的 IP 地址和路由器在同一个子网。
- 如果 BiGuard R1000 的 IP 地址已经更改，您并不知道当前的 IP 地址，请按住路由器背面的 Reset 按钮 6 秒重置路由器到出厂默认配置。路由器将重置 IP 地址到 192.168.1.254。
- 检查浏览器是否启用 Java，JavaScript 或者 ActiveX。如果您使用的是 IE 浏览器，点击**刷新**确保加载了 Java 小程序。
- 尝试关闭浏览器并且重新启动浏览器。
- 确保输入了正确了用户名和密码。用户名和密码是大小写敏感的，所以在输入这些信息的时候确保 CAPS LOCK 按键灯是不亮的。
- 尝试清除浏览器的缓存。若是用 IE 浏览器，参照如下操作：

1. 点击**工具 →Internet 选项**。
2. 在**常规**标签下，点击**删除**。
3. 进入**删除浏览的历史记录**窗口。
4. 确保勾选 **Internet 临时文件**选项，点击**删除**。
5. 在 **Internet 选项**中点击**确定**关闭窗口。

- 在 DOS 命令行中输入 **arp -d** 删除电脑上的 ARP （地址解析协议）列表。

禁用弹出窗口阻止程序

要使用 Web 配置界面，您需要禁用弹出窗口阻止程序。您可以禁用弹出窗口阻止程序，这个程序在 Windows XP SP2 中默认是启动的，或者为 BiGuard R1000 的 IP 地址创建一个排除条目。



NOTE: *以下的部分只介绍 IE 浏览器的设定内容。至于其他的浏览器设定，请参考浏览器的相关文档。*

禁用所有弹出窗口

在 IE 浏览其中，选择**工具** → **弹出窗口阻止程序**，然后选择**关闭弹出窗口阻止程序**。

您还可以在 Internet **选项**中的**隐私**标签下的**弹出窗口阻止程序**部分查看是否禁止了弹出窗口阻止程序。

1. 在 IE 浏览器中，选择**工具** →**Internet 选项**。
2. 在**隐私**标签下，去除**打开弹出窗口阻止程序**的复选框，然后点击**应用**保存设定。

启用弹出窗口阻止程序例外情况

参考以下步骤允许 BiGuard R1000 的弹出窗口阻止程序：

1. 在 IE 浏览器中，选择**工具** →**Internet 选项**。
2. 在**隐私**标签下，点击**设置**打开**弹出窗口阻止程序设置**窗口。
3. 输入路由器的 IP 地址。（默认是 192.168.1.254）
4. 点击**添加**可以添加这个 IP 地址到**允许的站点中**。
5. 点击**关闭**回到 Internet **选项**的隐私标签下。
6. 点击**应用**保存设定。

Java 脚本

如果 Web 配置界面不能够在浏览器中正确显示，请检查是否允许 Java 脚本。

1. 在 IE 浏览器中，选择**工具** →**Internet 选项**。
2. 在**安全标签**下点击**自定义级别**。
3. 在**脚本**部分，查看是否启用了**活动脚本**。
4. 确保启用了 **Java 小程序脚本**。
5. 点击**确定**关闭窗口。

Java 权限

以下的 Java 权限应该可以让 Web 配置界面能够正确显示：

1. 在 IE 浏览器中，选择**工具** →**Internet 选项**。
2. 在**安全标签**下点击**自定义级别**。
3. 在**微软 VM** 部分，确保一个选择 **Java 权限**的安全级别。
4. 点击**确定**关闭窗口。



NOTE: *如果安装了 Sun 公司的 Java，往下滚动到 Java (Sun)I 看看是否被选中。*

WAN 接口问题

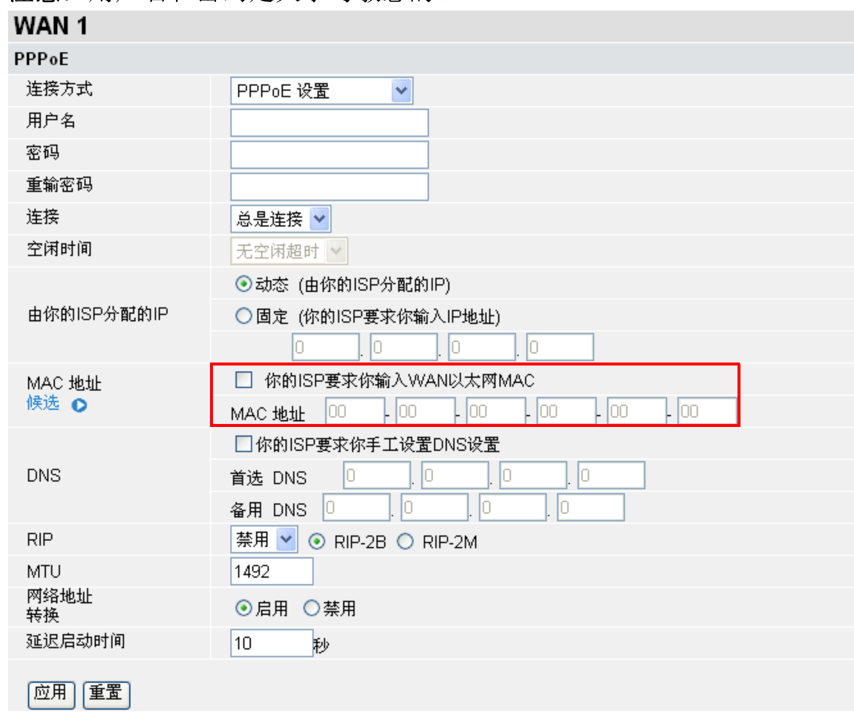
如果 WAN 接口有问题，请参考如下内容。

不能从 ISP 获得 WAN 接口的 IP 地址

不能从 ISP 获得 WAN 接口 IP 地址：

- 如果您在使用 PPPoE 或者 PPTP 封装，您需要 ISP 提供的用户名和密码。确保您输入了正确的**协议，用户名和密码**。

  注意：用户名和密码是大小写敏感的。



- 如果您的 ISP 需要 MAC 地址认证，请复制您的电脑网卡的 MAC 地址作为 BiGuard R1000 的 MAC 地址。点击**指定一个 MAC 地址 （MAC 复制）**，然后输入这个 MAC 地址。
- 如果您的 ISP 需要主机名称认证，配置 BiGuard R1000 使用您的电脑的设备名称。

Internet 服务提供商问题

除非您使用的是 ISP 分配的静态 IP 地址，BiGuard R1000 将需要从 ISP 获取一个 IP 地址用以访问 Internet。

连接到 BiGuard R1000 的时候不能访问 Internet

如果 BiGuard R1000 不能访问 Internet，首先确定路由器是否能够从 ISP 自动获得 WAN 接口的 IP 地址。

检查 WAN 接口的 IP 地址：

1. 打开浏览器输入一个外部站点 （例如 www.billion.com）。
2. 通过输入路由器的 IP 地址访问 Web 配置界面 （默认是 192.168.1.254）。WAN 的 IP 状态显示在状态界面。

WAN1	
连接方式	由静态IP设置连接
IP 地址	172.16.1.121
网络掩码	255.255.255.0
网关	172.16.1.254
DNS 服务器	172.16.1.254 202.102.24.35
启动时间	0: 0: 0: 7 (天:时:分:秒)

3. 检查 WAN 接口是否连接到 ISP。如果在没有显示上图的信息，路由器就没有从 ISP 成功获得 IP 地址。参考以下部分。

不能从 ISP 获得 IP 地址

如果不能获得 IP 地址：

1. 关闭 Cable 调制解调器或 DSL 调制解调器的电源。
2. 关闭 BiGuard R1000 的电源。
3. 等待 5 分钟，然后启动 Cable 调制解调器或 DSL 调制解调器。
4. 当调制解调器和 ISP 完成同步以后 （通常调制解调器上的 LED 灯会有所显示），打开路由器的电源。

如果您仍然不能获得 IP 地址：

- 您的 ISP 可能要求一个登录程序。联系您的 ISP 然后询问他们是否要求 PPPoE 或者其他类型的登录过程。
- 您的 ISP 要求您登录，检查用户名和密码是否输入正确。用户名和密码是大小写敏感的。
- 您的 ISP 可能要检查您的电脑的主机名。分配 ISP 帐户的电脑主机名作为路由器的设备名称。
- 您的 ISP 可能会检查您的电脑的 MAC 地址。告诉您的 ISP 您已经购买了一个新的网络设备，让他们设定路由器的 MAC 地址或者配置路由器复制允许的 MAC 地址。

可以获得 IP 地址，但是浏览器不能从 Internet 加载任何网页

- 您的电脑可能不能识别 DNS 服务器地址。手工配置您的电脑中的 DNS 地址。
- 您的电脑可能没有把路由器配置成为 TCP/IP 网关。

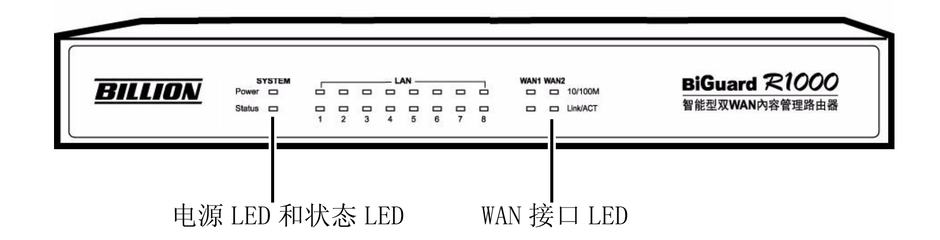
故障排错问答

这部分列出了 BiGuard R1000 操作中的一些常见问题，并给出了排错方法。

QUESTION: 当电源打开的时候，BiGuard R1000 的 LED 闪亮顺序如何？

ANSWER: 当 BiGuard R1000 在启动的时候，其 LED 灯的闪亮顺序如下：

- WAN 接口的 LED 灯闪两下。
- 电源和状态 LED 灯亮着。
- 在大约 30 秒的时间内，状态 LED 不亮了，说明系统已经启动完成。



QUESTION: BiGuard R1000 的默认用户名和密码是什么？

ANSWER: BiGuard R1000 的默认用户名和密码如下：

- 用户名：admin
- 密码：admin

QUESTION: BiGuard R1000 的出厂默认 LAN 接口 IP 地址是什么？

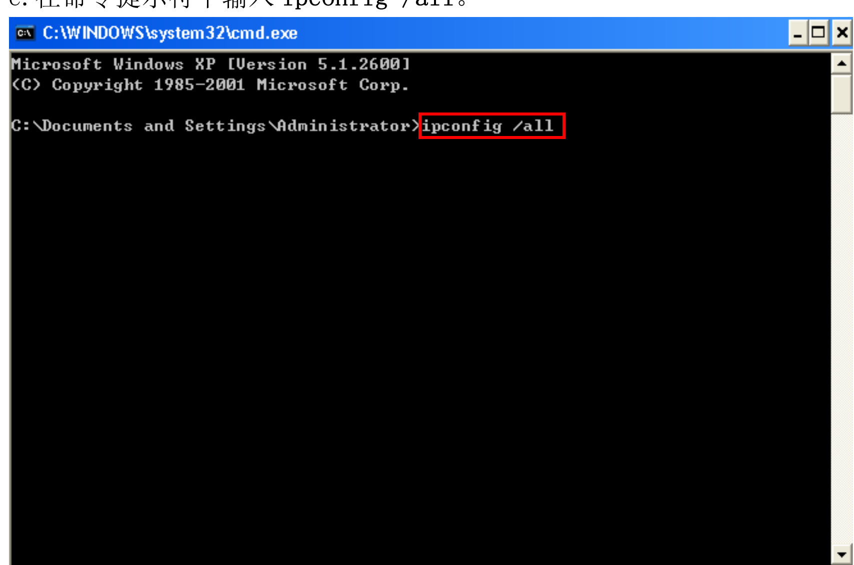
ANSWER: BiGuard R1000 的出厂默认 LAN 接口 IP 地址如下：

- IP 地址：192.168.1.254
- 子网掩码：255.255.255.0

QUESTION: 我记得BiGuard R系列路由器的LAN接口IP地址是192.168.1.254，但是我现在不能登录。我该怎么办？

ANSWER: 参考以下步骤：

1. 查看是否有别的电脑或路由器使用如下 IP 地址：192.168.1.254。
2. 如果您的电脑是自动分配 IP 地址的，请执行以下步骤：
   a. 在 Windows 操作系统中点击**开始** → **运行**。
   b. 在运行中输入 cmd，然后点击**确定**。
   c. 在命令提示符中输入 ipconfig /all。



3. 如果您的网络设定了静态 IP 地址，请确保正确设定了 IP 地址。
4. 如果步骤 1，2 和 3 不起作用，请关闭路由器，等待一分钟然后启动路由器执行步骤 1~3。
5. 如果您仍然不能登录，进行硬件重置恢复出厂默认配置。参考下面一个问题。

QUESTION: 如何重置 BiGuard R1000?

ANSWER: 有两种方法重置出厂默认配置：硬件重置和软件重置。

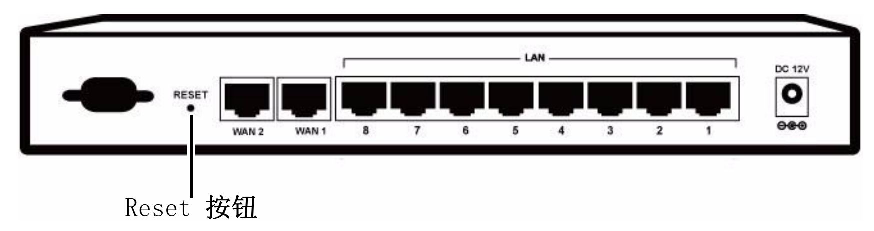
执行硬件重置

您可以通过按住路由器硬件 Reset 按钮恢复 BiGuard R1000 到出厂默认配置。



WARNING: 执行路由器的硬件重置将会擦除所有的设定并且恢复路由器到初始安装的状态。若要重置路由器而不擦除所有设定，可以进行软件重置。

若要执行硬件重置，按住 Reset 按钮 6 秒，等待状态 LED 灯闪烁。然后松开 Resset 按钮。



当完成硬件恢复出厂默认配置，状态 LED 灯就不亮了。

执行软件重置

若要执行软件重置，参考以下步骤。

1. 在菜单栏中点击**配置** → **系统** → **重启**。

FIGURE 87 重启界面



2. 选择**出厂设置**，重新启动以后使用出厂默认配置。
3. 点击**重启**就可以重启路由器。

一分钟以后，状态 LED 灯开始闪烁。在重置完出厂默认配置之后 LED 灯就不亮了。



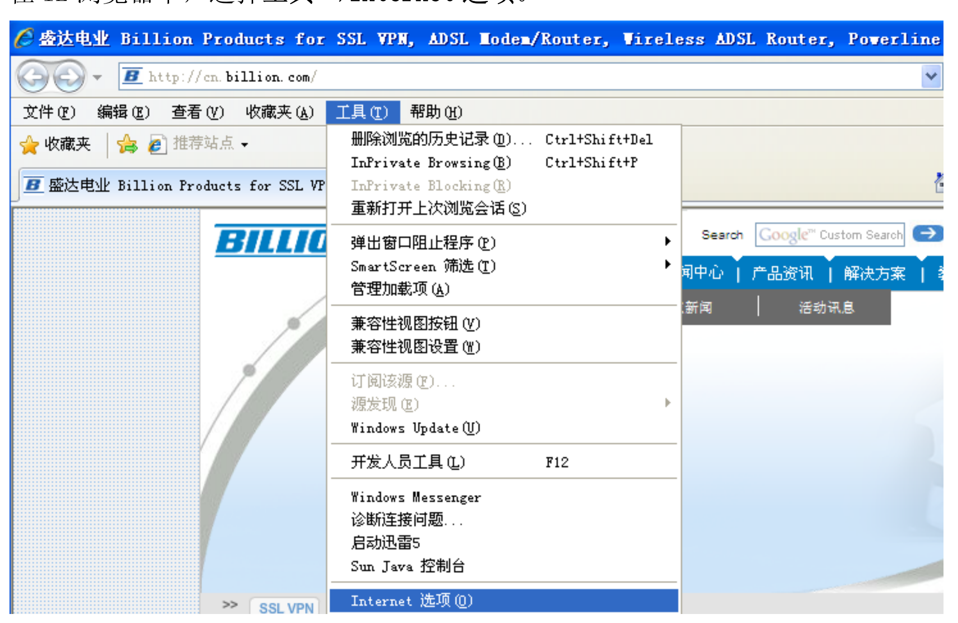
NOTE: *如果以上的步骤都不起作用，请联系经销商获取更多信息。*

QUESTION: 我升级路由器的韧件（Firmware）到最新版本，然后发现一些按钮或界面不能够正常显示。

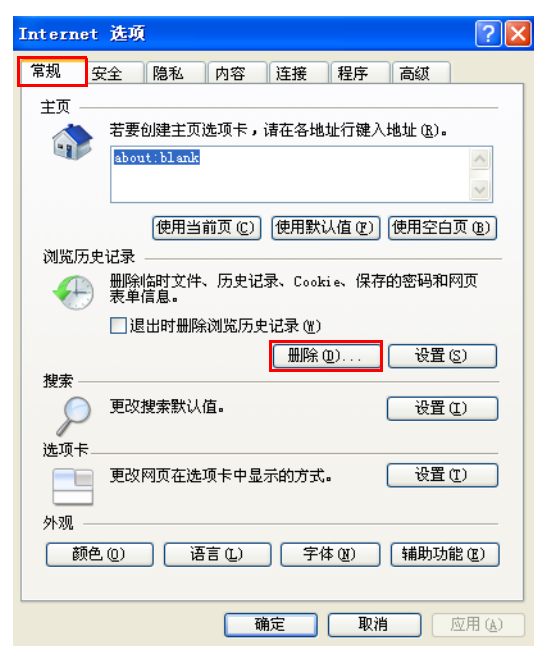
ANSWER: 可能是浏览器正在参考留在缓存中的数据。请清除缓存中的脱机数据，重新启动浏览器然后再试试。

按照如下步骤在 IE 浏览器中清除缓存：

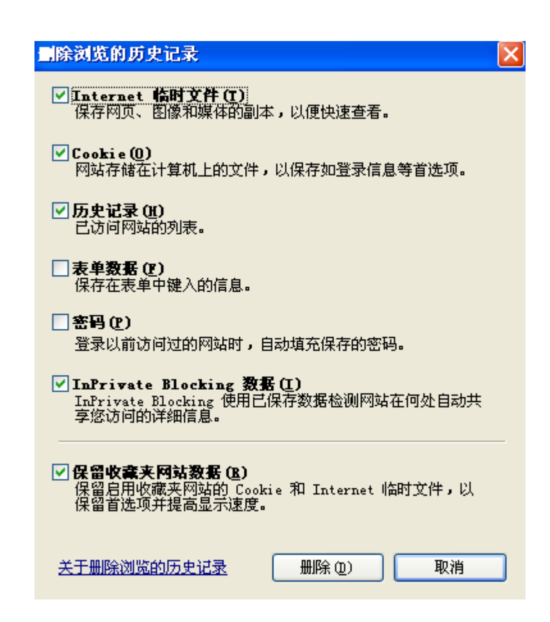
1. 在 IE 浏览器中，选择工具 →Internet 选项。



2. 在**常规**标签下点击**删除**。



3. 进入**删除浏览的历史记录**窗口，点击**删除**。


删除浏览的历史记录
Internet 临时文件 (T)
保存网页、图像和媒体的副本，以便快速查看。
Cookie (O)
网站存储在计算机上的文件，以保存如登录信息等首选项。
历史记录 (H)
已访问网站的列表。
表单数据 (F)
保存在表单中键入的信息。
密码 (P)
登录以前访问过的网站时，自动填充保存的密码。
InPrivate Blocking 数据 (I)
InPrivate Blocking 使用已保存数据检测网站在何处自动共享您访问的详细信息。
保留收藏夹网站数据 (R)
保留启用收藏夹网站的 Cookie 和 Internet 临时文件，以保留首选项并提高显示速度。
关于删除浏览的历史记录
删除 (D)
取消

BiGuard R1000FAQ

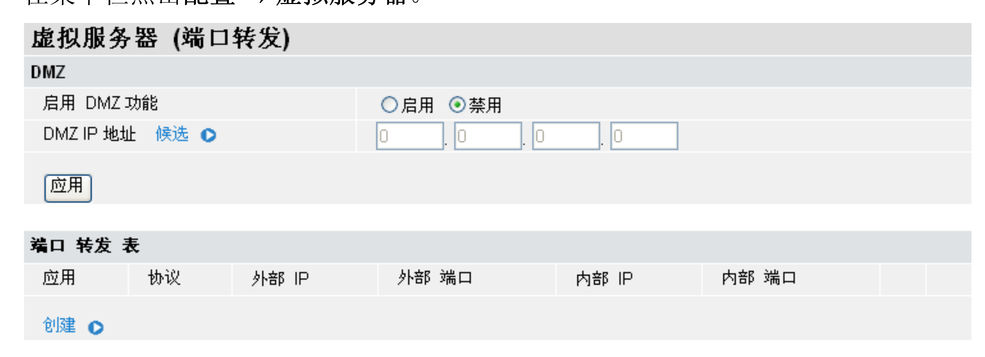
DMZ

QUESTION: 什么是 DMZ？如何设定 DMZ？

ANSWER: 非军事化区域（DMZ）接口提供一种方式，让公共服务器（如 FTP，Mail，Web 服务器等等）可以在被外部网络访问。这些公共服务器仍然可以从安全的 LAN 端访问到。它可以防护外部用户直接访问有公司数据的内部服务器。

若要在 BiGuard R1000 中设置 DMZ，请按照如下步骤：

1. 在菜单栏点击**配置** → **虚拟服务器**。



2. 选择**启用**可以启用 DMZ 功能。
3. 在 DMZ IP **地址**字段中输入内部应用服务器的 IP 地址，也可以点击**候选**进行选择。
4. 点击**应用**保存设定。

内容安全管理

QUESTION: 怎么样才能过滤 QQ 和 MSN 消息？

ANSWER: 可以使用 BiGuard R1000 的 IM 过滤功能来过滤 QQ 和 MSN 消息。：

1. 在菜单栏点击**内容安全管理** → **创建**。

创建一个组

配置

组过滤	⊙启用 ○禁用
组名	
开始IP地址	. . .
结束IP地址	. . . 增加
IP列表	删除
IM过滤列表	☐全选 ☑QQ ☑MSN ☐SKYPE ☐雅虎通 ☐ICQ ☐新浪UC ☐网易泡泡 ☐阿里旺旺
P2P过滤列表	☐严格限制 5 分钟 ☐全选 ☐迅雷 ☐BT ☐电骡/电驴 ☐快车 ☐酷狗 ☐QQ旋风
游戏过滤列表	☐全选 ☐魔兽世界 ☐泡泡堂 ☐梦幻西游 ☐跑跑卡丁车 ☐新浪Utgames ☐中国游戏中心 ☐QQ游戏 ☐MSN游戏 ☐ICQ游戏 ☐热血江湖 ☐劲舞团 ☐街头篮球 ☐联众 ☐浩方
股票过滤列表	☐全选 ☐国泰 ☐操盘手 ☐大智慧 ☐钱龙证券 ☐通达信 ☐同花顺 ☐证券之星 ☐指南针
视频过滤列表	☐全选 ☐PPLive ☐PPS网络电视 ☐QQ直播 ☐悠视网络电视 ☐迅雷看看 ☐土豆 ☐优酷 ☐Youtube ☐其他视频
计划 候选	**Always

应用 重置

2. 选择**启用**可以启用组过滤过滤功能。
3. 在**组名**中输入组名。
4. 在**开始 IP 地址**和**结束 IP 地址**中输入要进行 QQ 和 MSN 过滤的用户的 IP 地址。
5. 在 **IM 过滤列表**字段中勾选 **QQ** 和 **MSN**。
6. 点击**应用**保存设定。

QUESTION: 怎么样才能过滤迅雷，BT，电骡和网际快车下载软件？

ANSWER: 可以使用 BiGuard R1000 的 P2P 过滤功能来迅雷，BT，电骡和网际快车下载软件：

1. 在菜单栏点击**内容安全管理 → 创建**。

创建一个组

配置	
组过滤	⦿启用 ○禁用
组名	
开始IP地址	. . .
结束IP地址	. . . 增加
IP列表	删除
IM过滤列表	☐全选
	☐QQ ☐MSN ☐SKYPE ☐雅虎通 ☐ICQ ☐新浪UC ☐网易泡泡 ☐阿里旺旺
P2P过滤列表	☐严格限制 5 分钟
	☐全选
	☑迅雷 ☑BT ☑电骡/电驴 ☑快车 ☐酷狗 ☐QQ旋风
游戏过滤列表	☐全选
	☐魔兽世界 ☐泡泡堂 ☐梦幻西游 ☐跑跑卡丁车 ☐新浪Utgames ☐中国游戏中心 ☐QQ游戏 ☐MSN游戏 ☐ICQ游戏 ☐热血江湖 ☐劲舞团 ☐街头篮球 ☐联众 ☐浩方
股票过滤列表	☐全选
	☐国泰 ☐操盘手 ☐大智慧 ☐钱龙证券 ☐通达信 ☐同花顺 ☐证券之星 ☐指南针
视频过滤列表	☐全选
	☐PPLive ☐PPS网络电视 ☐QQ直播 ☐悠视网络电视 ☐迅雷看看 ☐土豆 ☐优酷 ☐Youtube ☐其他视频
计划 候选	**Always

应用 重置

2. 选择**启用**可以启用组过滤功能。
3. 在**组名**中输入组名。
4. 在**开始 IP 地址**和**结束 IP 地址**中输入要进行迅雷，BT，电骡和网际快车下载软件过滤的用户的 IP 地址。
5. 在**过滤列表**字段中勾选**迅雷**，**BT**，**电骡 / 电驴**和**快车**。
6. 点击**应用**保存设定。

防火墙

QUESTION: 如何设定防火墙规则阻挡 IP 地址为 192.168.1.100 的主机访问 Internet？

ANSWER: 在菜单栏中点击**网络安全管理** → **防火墙** → **包过滤**使用包过滤功能。请参照以下步骤。

1. 在菜单栏中点击**网络安全管理** → **防火墙** → **包过滤**。



包 过滤

包 过滤 表

ID	启用	动作	方向	源IP	目的IP	协议	源端口	目的端口

创建

2. 点击**创建**。

包 过滤

增加 过滤规则

字段	设置
ID	1
策略	⦿ 启用 ○ 禁用
匹配时作用	丢弃
方向	出站
源 IP	单一 地址；开始IP地址 192.168.1.100；结束IP地址 0.0.0.0；网络掩码 0.0.0.0
目的地 IP	任何；开始IP地址 0.0.0.0；结束IP地址 0.0.0.0；网络掩码 0.0.0.0
协议	任何
源 端口 范围 助手	1 ~ 65535
目的地 端口 范围 助手	1 ~ 65535
计划 候选	**Always
日志	○ 启用 ⦿ 禁用

应用 反向应用

ID	输入包过滤条目的 ID （只能输入 1-999 之间的数值）。
策略	勾选**启用**可以启用该包过滤条目。
匹配时作用	从下拉选项中选择动作应用的指定的数据包： • 丢弃：丢弃数据包。 • 转发：发送数据包。
方向	从下拉选项中选择包的流动方向： • **出站**：过滤从 LAN 接口到 WAN 接口的数据包。 • **入站**：过滤从 WAN 接口到 LAN 接口的数据包。
源 IP	在下拉选项中选择**任何**，**子网**，**IP 范围**或**单一地址**，然后在后面的地址和网络掩码字段输入相应的参数。
目的地 IP	在下拉选项中选择**任何**，**子网**，**IP 范围**或**单一地址**，然后在后面的地址和网络掩码字段输入相应的参数。
协议	在下拉选项中选择应用包过滤规则数据流量的协议，可以选择**任何**，TCP 或 UDP。
源端口范围	输入应用包过滤规则的数据流量的源端口范围。可以点击**助手**选择预定义的应用端口。
目的地端口范围	输入应用包过滤规则的数据流量的目的端口范围。可以点击**助手**选择预定义的应用端口。
计划	点击**候选**选择计划时间。
日志	勾选**启用**可以在过滤器运行的时候创建一个日志文件。

3. 点击**反向应用**保存设定，这样可以让包过滤规则应用在出站和入站两个方向。或者点击**应用**保存设定。

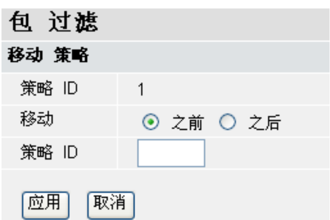


QUESTION: 包过滤序号 (#) 是什么意思？和优先级有关吗？

ANSWER: 包过滤序号 (#) 是包过滤策略的识别号，和优先级有关。



若要决定包过滤规则的优先级，可以点击**移动**，然后这条规则可以移动到更高或者更低的级别。



QUESTION: URL 过滤策略中支持哪些过滤？

ANSWER: 支持如下的 URL 过滤功能：

- 关键字过滤
- 域名过滤
- 限定 URL 特性 （包括阻塞 Java 小程序，阻塞 ActiveX，阻塞 Cookies，阻塞 Proxy 代理服务器和 IP 地址阻塞上网 ）

QUESTION: URL 过滤策略中的关键字过滤是什么？怎么使用？

ANSWER: 关键字过滤是一种阻塞访问任何含有用户自定义关键字的 URL 的一种技术。

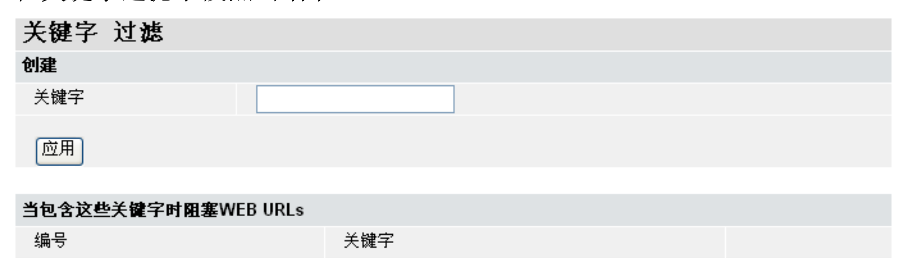
用户若要定义关键字过滤用以阻塞相关的 Web 站点。

首先，用户必须设定关键字过滤网络对象。

1. 在菜单栏中点击**网络安全管理 → 防火墙 →URL 过滤**。



2. 在**关键字过滤**字段点击**细节**。



3. 在**关键字**字段输入关键字。
4. 点击**应用**，然后这个关键字过滤规则就会列在**当包含这些关键字时阻塞 WEB URLs** 中。
5. 可以按照这种方式增加更多的关键字过滤规则。



6. 返回到创建 URL 过滤界面，在 **URL 过滤**字段选择**启用**，在**关键字过滤**字段勾选**启用**。

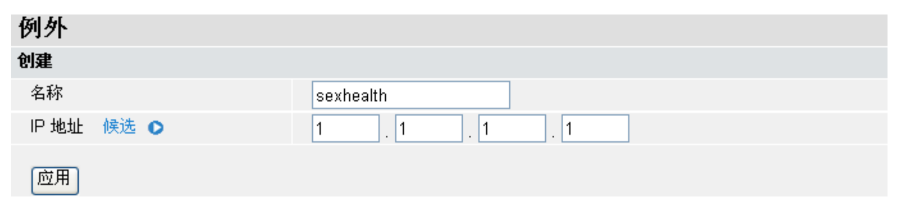


7. 点击**应用**保存设定。



NOTE: *过滤器将会阻塞 URL，例如 www.sexpicture.com 和其他相关的在域名中有 sex 的 URL。然后它不仅仅阻塞了潜在的危害，也会阻塞了例如 www.sexhealth.com 的域名。您可以让这种域名不在阻塞的列表中。*

如果您想在 URL 过滤策略中排除一些 IP 地址，点击例外列表中的**创建**，然后在 IP **地址**字段中输入 IP 地址，或者通过点击**候选**选择一个 IP 地址。



QUESTION: URL 过滤策略中的域名过滤是什么？怎么使用？

ANSWER: 域名过滤是一种为阻塞特定域名地址设计的防火墙功能。

如果用户想阻塞 www.sex.com 的访问。请参考以下步骤：

1. 在菜单栏中点击**网络安全管理 → 防火墙 →URL 过滤**。

URL 过滤

配置

URL 过滤	○ 启用 ⦿ 禁用
关键字 过滤	☐ 启用 细节
域名过滤	☐ 启用 细节
	☐ 禁止访问信任域名以外的域名
限制URL特性	☐ 阻塞 Java Applet
	☐ 阻塞 ActiveX
	☐ 阻塞 Web 代理
	☐ 阻塞 Cookie
	☐ 用IP地址阻塞上网
日志	☐ 启用

应用

例外列表

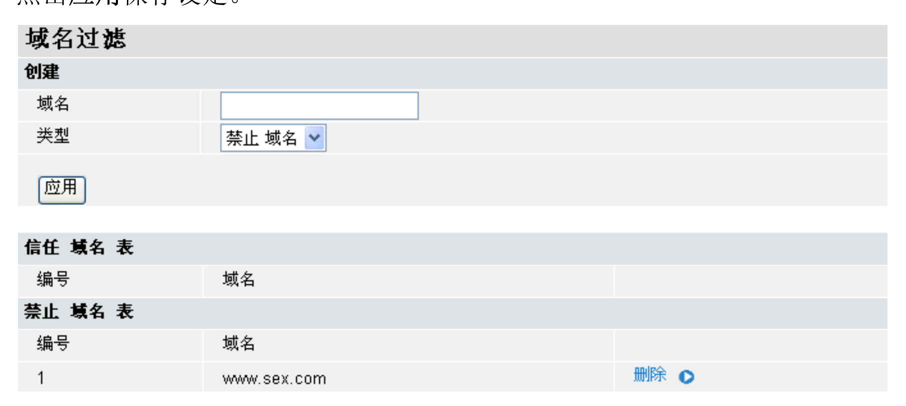
名称	IP 地址		

创建

2. 在**域名过滤**字段点击**细节**。



3. 然后在**域名**字段中输入域名，例如 www.sex.com。
4. 在**类型**下拉选项中选择**禁止域名**。
5. 点击**应用**保存设定。



如果你想允许某些带有用户定义域名的域名，例如 www.sexhealth.com。

6. 在**域名**字段中输入域名，例如 www.sexhealth.com。
7. 在类型下拉选项中选择**信任域名**。
8. 点击**应用**保存设定。



9. 返回到创建 URL 过滤界面，在 **URL 过滤**字段选择**启用**，在**域名过滤**字段勾选**启用**。



10. 点击**应用**保存设定。

QUESTION: 在域名过滤字段中中 “禁止访问信任域名以外的域名”选项的作用是什么？怎么使用？

ANSWER: **禁止访问信任域名以外的域名**阻止所有的 Web 数据流除了用户定义的信任域名的数据流。

允许用户访问 www.billion.com 的 URL，请参考以下步骤：

1. 按照上面问题的步骤指定 www.billion.com 作为信任域名。

域名过滤

创建

域名	
类型	禁止 域名

应用

信任 域名 表

编号	域名	
1	www.billion.com	删除

禁止 域名 表

编号	域名	

2. 返回到创建 URL 过滤界面，在 **URL 过滤**字段选择**启用**，在**域名过滤**字段勾选**启用**和**禁止访问信任域名以外的域名**。



3. 点击**应用**保存设定。

QUESTION: 在限制特性中什么是阻塞 Java 小程序，阻塞 ActiveX?

ANSWER: 阻塞 Java 小程序和 ActiveX 可以阻塞 HTML 访问文件中潜在的有害内容，例如 .js 文件，.class 文件，.ocx 文件或 .cab 文件。

下载恶意的 Java 小程序和 Java 脚本可以窃取，删除或者更改信息，危害安全以及突破用户系统。另外，buggy 小程序会影响性能并且浪费网络资源。一旦启用了这种功能，恶意的代码不能执行除非关闭了该功能。

在设置限定 Java 小程序和 Java 脚本以前，您必须首先创建限定 URL 特性网络对象。请参考以下步骤：

1. 在菜单栏中点击**网络安全管理** → **防火墙** →**URL 过滤**。



2. 在 URL **过滤**字段选择**启用**，在**限制 URL 特性**字段勾选**阻塞** Java Applet 和**阻塞** ActiveX 选项。
3. 点击**应用**保存设定。

QUESTION: 在限定特性中什么是阻塞 Proxy 代理服务器？

ANSWER: 这种策略阻塞用户访问设定的代理服务器，防止用户通过代理服务器绕过规则使用 Internet 连接。

若要设定阻塞 Proxy 代理服务器，请参考以下步骤。

1. 在菜单栏中点击**网络安全管理** → **防火墙** →**URL 过滤**。



2. 在 URL **过滤**字段选择**启用**，在**限制 URL 特性**字段勾选**阻塞 Web 代理**选项。
3. 点击**应用**保存设定。

QUESTION: 在限定特性中什么是阻塞 Cookies?

ANSWER: 这个策略阻塞保存和阅读 cookies。不论是安全还是不安全的网站都不可以使用 cookies 功能。

若要阻塞 cookies，请参考以下步骤。

1. 在菜单栏中点击**网络安全管理 → 防火墙 →URL 过滤**。



2. 在 **URL 过滤**字段选择**启用**，在**限制 URL 特性**字段勾选**阻塞 Cookie** 选项。
3. 点击**应用**保存设定。

QUESTION: 在限定特性中什么是通过 IP 地址阻塞上网?

ANSWER: 启用通过 IP 地址阻塞上网策略让用户只能通过域名访问网站。

若要阻塞 IP 地址上网，请参考以下步骤。

1. 在菜单栏中点击**网络安全管理 → 防火墙 →URL 过滤**。



2. 在 URL **过滤**字段选择**启用**，在**限制 URL 特性**字段勾选用 **IP 地址阻塞上网**选项。
3. 点击**应用**保存设定。

QUESTION: 什么是 URL 过滤策略中的例外列表？

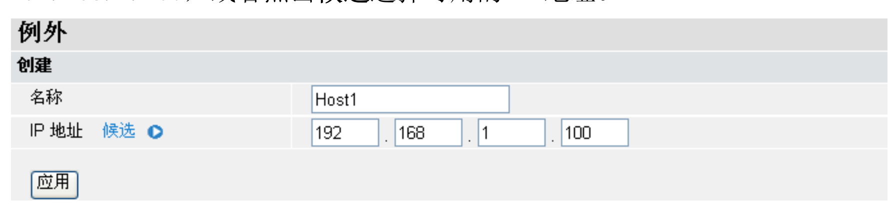
ANSWER: 例外列表就是一个选项可以从 URL 过滤策略中排除的 IP 地址。

用户如果想把 192.168.1.100 的 IP 地址放在例外列表中，可以参考以下步骤。

1. 在菜单栏中点击**网络安全管理 → 防火墙 →URL 过滤**。



2. 点击**创建**可以创建例外 IP 地址。
3. 在**名称**字段中输入名称，如 Host1，在 **IP 地址**字段中输入排除 IP 地址，如 192.168.1.100，或者点击**候选**选择可用的 IP 地址。



4. 点击**应用**保存设定。



5. 可以点击**删除**移除例外 IP 地址。

QUESTION: 什么是以太网 MAC 地址过滤？怎么使用？

ANSWER: BiGuard R1000根据允许拒绝地址列表检查MAC地址以决定是允许还是拒绝请求。请参考以下步骤。

用户如果想让 00:11:11:11:11:11 的 MAC 地址不能访问 Internet。

1. 在菜单栏中点击**网络安全管理** → **防火墙** →**LAN MAC 过滤**。



2. 在以太网 MAC 过滤界面中点击**创建**。



3. 在**策略**字段勾选**启用**可以启用该 LAN MAC 地址过滤规则。
4. 在**动作**下拉选项中选择**丢弃**。
5. 在 **MAC 地址**字段输入 MAC 地址或者点击**候选**选择可用的 MAC 地址。

Ethernet MAC 过滤

创建规则

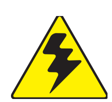
策略	⦿ 启用 ○ 禁用
匹配时作用	丢弃
Mac 地址 候选	00:11:11:11:11:11
绑定 IP	○ 启用 ⦿ 禁用
IP 地址	. . .
日志	○ 启用 ⦿ 禁用
应用	

6. 点击**应用**保存设定。



7. 点击**应用**保存设定。

如果用户想阻塞所有的 MAC 地址访问 Internet，除了 00:11:11:11:11:11。



WARNING: 当配置了默认的以太网 MAC 过滤器规则去丢弃，请先添加管理员的 MAC 地址的转发规则。否则，管理员将不能访问 BIGUARD R1000。

1. 在菜单栏中点击**网络安全管理 → 防火墙 →LAN MAC 过滤**。



2. 在以太网 MAC 过滤界面中点击**创建**。



3. 在**策略**字段勾选**启用**可以启用该 LAN MAC 地址过滤规则。

4. 在**动作**下拉选项中选择**转发**。
5. 在 **MAC 地址**字段输入 MAC 地址或者点击**候选**选择可用的 MAC 地址。



6. 点击**应用**保存设定。



7. 在**缺省策略**下选择**丢弃**。



8. 点击**应用**保存设定。

QUESTION: 为什么我从 Internet 无法 Ping 通 BiGuard R1000 的 WAN 接口 IP 地址？

ANSWER: 确保禁用了阻塞 WAN 请求功能。

在菜单栏中点击**网络安全管理** → **防火墙** → **阻塞 WAN 请求**可以配置阻塞 WAN 请求。

FIGURE 88 阻塞 WAN 请求界面

阻塞WAN请求	
启用以阻止来源于Internet，例如骇客的攻击。	
阻塞WAN请求	⦿启用 ○禁用
阻塞WAN ICMP请求	⦿启用 ○禁用
应用	

阻塞 WAN 请求	启用该功能可以阻塞 WAN 接口上的所有数据包的请求。
阻塞 WAN ICMP 请求	启用该功能可以阻塞 WAN 接口上的 ICMP 数据包的请求，也就是无法 Ping 通 WAN 接口。

点击**应用**保存设定。

远程访问

QUESTION: 如何配置 BiGuard R1000 的远程访问设定？

ANSWER: 在菜单栏中点击**配置** → **系统** → **远程访问**可以配置远程访问功能。

1. 点击**远程访问**启用远程访问功能。

FIGURE 89 启用远程访问界面

远程访问	
远程访问 功能	
动作	○启用 ⦿禁用
* HTTPS 端口	443
*：这项设置在你存入闪存并重启路由器后会有效	
应用	

远程访问 表	
编号	IP 地址
创建	

远程访问功能	
动作	选择启用可以允许远程访问。
HTTPS 端口	可以自定义 HTTPS 端口用于远程访问，默认端口是 443。
远程访问表	
编号	远程访问规则条目的编号。

IP 地址	允许远程访问的 IP 地址。

2. 点击**创建**进入配置远程访问主机的界面。

FIGURE 90 配置远程访问主机界面

远程访问

你可以对这台网络设备远程管理 (HTTPS).

允许远程访问由	⦿每人 (每人)
	○只这台PC: . . .
	○来自这个子网的PC:

应用

每人	允许任何人访问该设备。
只这台 PC	只允许指定的一台 PC 访问该设备。
来自于这个子网的 PC	只允许指定子网的 PC 访问该设备。

3. 点击**应用**保存设定返回启动远程访问界面。

远程访问

远程访问 功能

动作	⦿ 启用 ○ 禁用
* HTTPS 端口	443

*: *这项设置在你存入闪存并重启路由器后会有效*

应用

远程访问 表

编号	IP 地址		
#1	ANY	编辑	删除

创建

4. 点击应用**保存**设定。



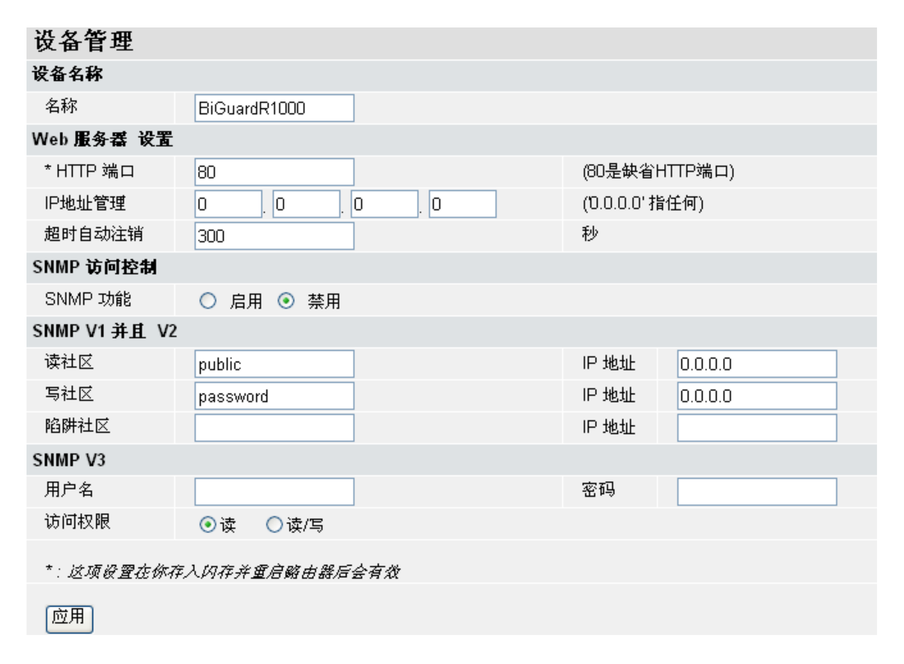
WARNING: 如果允许远程访问控制，建议您配置指定的 IP 地址，以供管理员使用。

QUESTION: 什么是自动登出计时器？

ANSWER: 在帐户配置界面的**超时自动注销**字段中的默认数值是300秒。如果在Web管理界面的空闲时间超过这个数值，帐户将被自动登出 BiGuard R1000。

您可以参考以下步骤配置自动登出计时器。

1. 在菜单栏中点击**配置** → **高级** → **设备管理**。



2. 在**超时自动注销**字段中，输入时间（以秒计算），可以决定帐户在空闲一段时间后自动登出。
3. 点击**应用**保存设定。

QUESTION: 是否能通过 WAN 接口远程升级韧件（Firmware）？

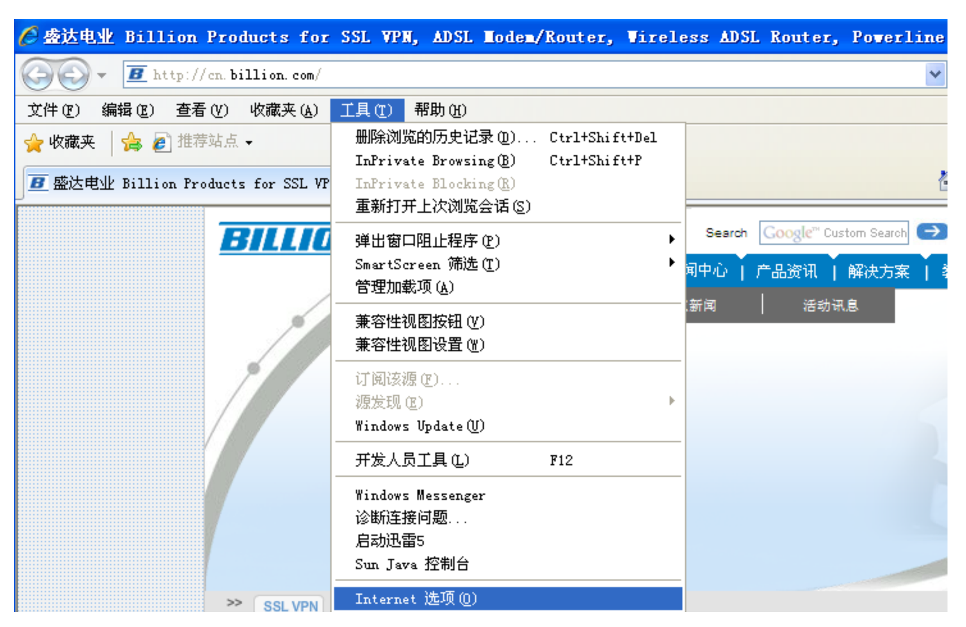
ANSWER: 可以远程升级，不过 Billion 不建议这样做。因为在不同的地区 Internet 服务的可靠性是不同的。连接随时都有可能中断，因此导致韧件升级失败。

QUESTION: 我升级路由器的韧件（Firmware）到最新版本，然后发现一些按钮或界面不能够正常显示。

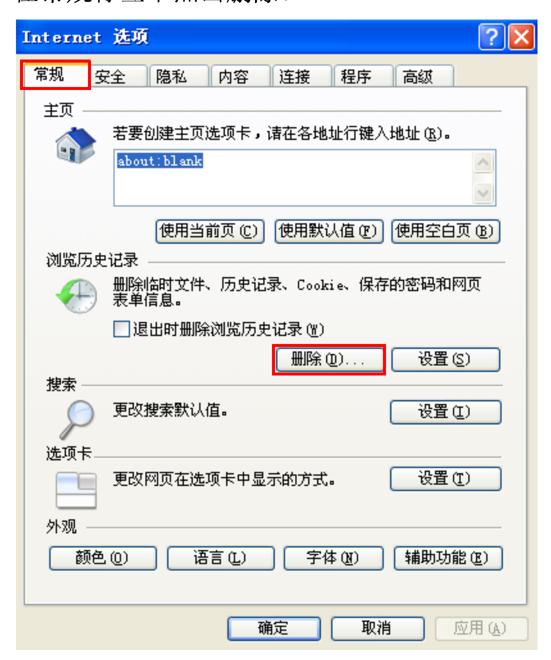
ANSWER: 可能是浏览器正在参考留在缓存中的数据。请清除缓存中的脱机数据，重新启动浏览器然后再试试。

按照如下步骤在 IE 浏览器中清除缓存：

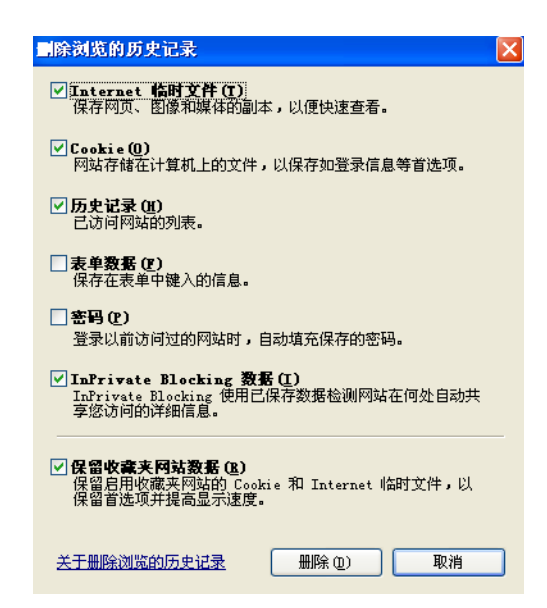
1. 在 IE 浏览器中，选择**工具** →**Internet 选项**。



2. 在**常规**标签下点击**删除**。



3. 进入**删除浏览的历史记录**窗口，点击**删除**。



SNMP

QUESTION: BiGuard R1000 支持哪些 SNMP MIB?

ANSWER: BiGuard R1000 支持下列 MIB:

- RFC1213(MIB-II)
- System 组
- Interfaces 组
- Address Translation 组
- IP 组
- ICMP 组
- TCP 组
- UDP 组
- SNMP 组

QUESTION: BiGuard R1000 支持哪些 Web 浏览器。

ANSWER: 强烈建议使用下列浏览器:

- IE 6.0SP1 （支持微软 IE 5.01 或更新版本）
- Mozilla 1.7.1 或更新版本
- Firefox 1.0.6 或更新版本
- Opera 8.02 或更新版本
- Safari 1.3.1 或更新版本

QUESTION: 需要在浏览器上激活什么才能成功连接 BiGuard R1000?

ANSWER: 下面列出的浏览器中选项需要启用才能成功连接:

- Cookies
- 弹出窗口
- Java
- Java 脚本
- ActiveX

QUESTION: 需要什么版本的 Java？

ANSWER: 您需要安装 Sun JRE 1.31 或更新版本（可以在 http://www.java.com 下载）才能使用 BiGuard R1000 的功能，但是我们建议使用 1.5 或更新版本。如果您遇到 RDP5 的 Java 组件问题，请升级到 Java 的最新版本。

网络基础

IP 地址

全世界使用 TCP/IP 进行互联的网络必须确保数据能够传送到正确的目的地，这就需要互联网中的每一台计算机设备都有一个唯一的标识符。这个标识符就是众所周知的 IP 地址。互联网协议（IP）使用 32 位地址结构，一般用点分十进制的形式表示。

一个典型的 IP 地址是：*198.25.12.8*

这个 32 位的地址包括两部分。第一部分标识了了网络位，而第二部分标识了主机位。至于如何划分这两部分，取决于需要的地址范围和具体应用。

IP 地址分成五类，每个类的 IP 地址网络位和主机位都有所不同，使得一个网络中存在多台主机成为可能。TCP/IP 软件能够通过读取地址类型前面的唯一的位模式来识别地址类。一旦识别了地址类，软件就能正确的确定主机位。在这种结构下，IP 地址能唯一地识别每个网络和主机节点。

子网掩码

每个地址类可以细分成两个部分 （网络地址和主机地址）。与 IP 地址相结合的子网掩码能够表示出这两个部分的区别。当子网掩码和 IP 地址相配合的时候，32 位的子网掩码是根据 IP 地址来确定的。例如，A 类 ,B 类和 C 类的子网掩码分别是 255.0.0.0，255.255.0.0 和 255.255.255.0。

与点分十进制不同，子网掩码可以根据 IP 地址的网络位书写。把子网掩码和 IP 地址写在一起的时候使用反斜杠 （/）。例如，典型的 C 类地址可以写成 192.168.234.245/24，表示这个子网掩码中前 24 位是 1，后 8 位是 0。（11111111 11111111 11111111 00000000）

变长子网掩码

变长子网掩码使得 IP 地址的网络位可以分成多个物理子网。这些较小的子网在连接路由器的两端时能够有效地利用地址。这种技术特别适用在小型的网络环境中，例如小型办公局域网。

一个 B 类的地址可以提供 16 位的主机位，能够容纳 65535 个节点。因为大多数的机构都不会需要如此多的节点数，那么就可以使用变长子网掩码重新分配网络位和主机位。

一个 B 类地址可以分成多个 C 类地址。例如，172.20.0.0 的 IP 地址可以增加 8 位网络位，使其节点地址最大为 254。IP 地址 172.20.52.212 将被识别为网络位是 172.20.52，主机位是 212。

除了扩展可用地址的数量，这种技术还能够允许网络管理员为网络设计一个地址方案。还可用于区分网络中的地理位置或机构中的其他部门。

私有 IP 地址

不与 Internet 相连的时候，在本地网络的主机可以分配没有冲突的 IP 地址。然而，Internet 号分配机构 （IANA）保留了一些 IP 地址段给私有网络使用。包括：

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.16.255.255

192.168.0.0 - 192.168.255.255

您可以使用这些地址分配到私有网络中。

网络地址转换 （NAT）

传统上，多台计算机需要同时访问 Internet 的时候需要从 Internet 服务提供上 （ISP）获取多个 IP 地址。这样做不但成本很高，而且各个计算机使用的 IP 地址也很有限。相反，BiGuard R1000 使用网络地址转换 （NAT）让多台计算机同时访问 Internet 的时候可以使用相同的公网 IP 地址。这种方式转换了多个内网 IP 地址到一个公网 IP 地址上。这个公网 IP 地址可以是固定的或动态的，这取决于连接 Internet 的方式，内网的 IP 地址也可能是私有的或者是注册的。

NAT 还能够提供类似于防火墙防护的功能，使得内部网络不会暴露在公共的 Internet 上。所有数据流都可以由路由器进行转发，这意味着给您的网络增添了安全性，防止黑客入侵。如果在内部网络上的特殊计算机需要让外部计算机访问，您可以使用端口转发技术，也就是虚拟服务器技术来实现。若要具体了解该项技术，请参考 BiGuard R1000 的虚拟服务器功能。

动态主机配置协议 （DHCP）

如果内网的计算机要访问 Internet，那么每台计算机都要配置一个 IP 地址，网关，以及一个或多个 DNS 服务器地址。较之于给每台计算机手工配置地址信息，您可以用动态主机配置协议 （DHCP）服务器来更好地配置地址信息。这样内网的计算机都可以自动从 DHCP 服务器获得 IP 地址。另外，例如网关和 DNS 地址也可以由 DHCP 服务器分配。当连接到 ISP 的时候，BiGuard R1000 可以作为 DHCP 客户端，自动从 ISP 获得 IP 地址，子网掩码，网关和 DNS 服务器地址。

路由器基础

什么是路由器？

路由器是一种可以对网络数据包进行路由寻址的设备。路由器至少需要连接两个网络。通常，路由器连接内部网络和外部网络。路由器连接两个或多个网络。路由器使用使用路由协议进行彼此通讯确定网络拓扑，通过查看数据包头和路由表决定转发数据包的最佳路径。

路由器因性能和标准不同而不同，他们可以支持不同的 WAN 接口的类型，以及不同的路由协议的类型。BiGuard R1000 提供简便实用的方法让中小企业可以连接他们的网络。

为什么使用路由器？

如今，高带宽可以简单廉价地在内部网络中使用，在内部网络和外部网络之间的高带宽也不那么贵。若要有效地使用 Internet 慢速连接 （Internet 访问常常是较慢的 WAN 连接，例如 Cable 调制解调器或 DSL 调制解调器），路由器可以作为一种选择和传输数据到 Internet 的机制。通过使用路由器，机构可以享用廉价的 Internet 访问，同时享用高速地内部网络。

路由信息协议 （RIP）

路由信息协议 （RIP）是一种内部网关协议指定了路由器如何交换路由表信息。路由器彼此可以通过 RIP 进行定期更新。

BiGuard R1000 支持 RIP 路由协议。RIP 同样支持变长子网掩码和组播协议。大多数的应用程序不需要 RIP 路由协议。

防火墙基础

什么是防火墙？

防火墙可以防止未授权的 Internet 用户访问连接到 Internet 的私有网络。所有进出内部网络的数据流都通过防火墙，然后防火墙检查每个消息块，看是否符合一定的安全标准。使用 NAT 的路由器，防火墙增加了处理外部 Internet 入侵攻击的功能。当检测到入侵攻击的时候，防火墙可以配置记录入侵日志，然后将事件通知给管理员。利用这些信息，管理员可以与 ISP 协同工作对黑客采取行动。防火墙可以防护一些攻击类型，丢弃入侵者的数据包，因此可以把黑客拒在私有网络之外。

状态封包检测 （SPI）

BiGuard R1000 使用状态封包检测 （SPI）去防护网络入侵攻击。不像少数尖端的 Internet 共享路由器，SPI 能够确保防火墙在网络层截取数据包进行过滤，并且通过与网络连接有关的状态信息进行分析。BiGuard R1000 通过查看连接状态分析用户层的应用程序，例如 Web 浏览器和 FTP 的复杂网络数据流模式。

所有状态信息都保存在一个中央的缓存中。防火墙依靠这些状态对穿过防火墙的数据流进行分析，然后决定是否允许穿过防火墙。

拒绝式服务攻击 （DoS）

黑客可能会通过拒绝式服务 （DoS）攻击让您的网络无法正常工作或通讯。这种攻击方法很简单，仅仅是让您的网络承受太多不能承受的数据请求。一种更加高级的攻击试图探测您的路由器或网关使用的操作系统漏洞。一些操作系统可能在被发送了一个错误长度的数据包就不行了。

为什么使用防火墙？

通过一个连接到 Internet 的路由器，黑客有机会访问或者中断您的网络。一个简单的 NAT 路由器可以提供一个基本的防护，对外部 Internet 网络隐藏内部网络。然后，仍然有很多职业黑客可以获取您的网络信息或中断您网络的 Internet 访问。BiGuard R1000 可以通过内置的防火墙功能提供额外的防护以防护这种攻击。

技术规格

可扩展性及弹性

- 双 WAN 接口
- 中国电信和中国联通智能路由
- 负载平衡
    - 增强型宽带出站及入站传输的负载平衡
    - 域名（DNS）入站负载平衡
- 协议捆绑
- 自动线路备份

智能网络管理工具

- WAN 流量统计
- LAN 流量统计
- 连接统计及限制
- 流量管理（QoS）控制
    - 支持 DiffServ approach
    - 基于 IP 协议，连接端口数量
      以 IP 地址为基础的流量优先处理及带宽管理
    - 基于 IP&MAC 地址控制

上网行为管理

- 即时通讯过滤：QQ，MSN，Skype 等
- P2P 过滤：迅雷，电骡，BT 等
- 其他应用过滤：视频娱乐，网络游戏，股票

基于 Web 的管理

- 操作简便的 Web 界面
- 通过 Web 界面升级韧件 （Firmware）
- 通过 HTTP 的本地和远程管理

IPTV 应用

- IGMP Snooping 影像服务
- 虚拟局域网（VLAN）
- 流量管理（QoS）

网页内容过滤

- URL 过滤设定可预防用户在互联网上访问某些站点
- 阻塞 Java 小程序 /ActiveX/Web 代理 / 使用 IP 地址访问 /Cookies

防火墙

- 状态封包检测（SPI）及预防拒绝式服务（DoS）攻击
- 信息包过滤不允许入站（WAN）出站（LAN）互联网访问
- E-mail 监测及日志攻击
- MAC 地址过滤

网络协议和特性

- 系统日志
- PPPoE，PPTP 及 DHCP 客户端连接至 ISP
- NAT，静态路由及 RIP-1/2
- 动态域名解析系统（DDNS）
- BiGuard 客户专享 DDNS 服务
- 虚拟服务器（Virtual Server）及隔离区（DMZ）
- DHCP 服务器
- 网络时间协议（NTP）
- SMTP 客户端
- 支持 SNMP
- 支持 SIP 穿透（Pass-through）
- 支持 IGMP snooping&IGMP Proxy
- 支持基于端口的 VLAN
- 支持多个 WAN 别名及 LAN 子网

硬件规格

物理接口

- 2 x WAN 接口 （10/100Mbps，MDI/MDIX）
- 8 x LAN 接口 （10/100Mbps，MDI/MDIX）

实体规格

- 尺寸 （长，宽，高）：19 英寸 x 6.54 英寸 x 1.65 英寸
  (482 毫米 x 166 毫米 x 42 毫米 含支架）
  (250 毫米 x 166 毫米 x 42 毫米 不含支架）

电源规格

- 输入：12V DC，1A

作业环境

- 工作温度： 0 ~ 40 ° C
- 存储温度： -20 ~ 70 ° C
- 湿度：20 ~ 95% 非冷凝

术语表

术语表

下表列出了常用的网络专业术语，仅供参考。

术语	定义
接入点	接入点是连接到以太网集线器或服务器的无线局域网接入点。用户可以在接入点支持的范围内漫游，他们的无线设备从一个接入点过渡到另一个接入点。
认证	认证指的是指对传输信息的完整性的确认。
DMZ （非军事化区）	非军事化区 （DMZ）是网络的一个部分，其既不是内网的一部分也不是外部 Internet 网的一部分。通常放在两个防火墙中间或者在防火墙的单独一端，在该区域中放置服务以供外部网络的用户访问。
Beacon Interval	指的是接入点为了同步无线局域网而发送的数据包间隔时间。
DHCP （动态主机配置协议）	DHCP （动态主机配置协议）可以自动分配 IP 地址到 TCP/IP 网络，可以代替手工配置 IP 地址。
DNS （域名解析系统）	DNS （域名解析系统）可以进行 IP 地址和域名的相互解析。
域名	域名是 Internet 站点地址的别名，为了方便人们记忆而产生的。
双 WAN 接口	双 WAN 接口可以做在线备份和负载均衡，不但可以增强网络的可靠性，而且可以增加可用带宽。
过滤器	过滤器可以定义特定的数据类型。例如，路由器可以使用过滤器定义的数据类型对数据包进行识别，然后对该数据包进行适当的操作。
防火墙	防火墙可以保护网络安全，防止黑客入侵和非授权访问。防火墙使用过滤器防止传输不必要的数据包。防火墙通常用在隔离机构的 Web 服务器和内部网以及外部 Internet 网络的访问。
韧件（Firmware）	韧件 （Firmware）指的是设备的操作系统，存放在设备的 Flash 存储器中。
分段	指的是在传输过程中对数据包的分割。
FTP （文件传输协议）	FTP （文件传输协议）用于在 TCP/IP 网络中传输文件，特别是用于传输大型文件或上传 HTML 页面到 Web 站点给 Web 服务器。
网关	网关是计算机转换协议使得不同的网络，应用程序和操作系统能够交换信息。
主机名	计算机或网络设备的名称，通常是 NetBios 名。
HTTP （超文本传输协议）	HTTP （超文本传输协议）是一种通讯协议，可以连接到 www （万维网）服务器。HTTP 建立到 Web 服务器的连接，然后传输 HTMP 页面给客户端浏览器 （例如 Windows IE）。HTTP 地址总是以 http:// 开头。例如 http://www.billion.com
ICMP （Internet 控制消息协议）	ICMP （Internet 控制消息协议）是一种 TCP/IP 协议，用于在局域网中发送错误和控制消息。（例如路由器使用它通知发送者目标不可达）
IP （Internet 协议）	IP （Internet 协议）是 TCP/IP 协议簇中位于网络层的协议。其包含一个网络地址并且允许消息路由到不同的网络。然而，IP 不保证消息可靠传输，需要依靠 TCP 提供。

术语	定义
IP 地址	IP 地址指的是使用 TCP/IP 协议的计算机的地址。每个客户端和服务器必须有唯一的 IP 地址。客户端要么配置永久地址要么通过 DHCP 分配动态地址。IP 地址可以写成四段点分十进制的样子，例如 211.23.181.189。
ISP（Internet 服务提供商）	ISP 是一个提供 Internet 接入服务的机构，可以提供例如 ISDN，ADSL 和专线等连接。
LAN （局域网）	LAN （局域网）是能够覆盖较小地理区域用户的网络，例如公司大楼。局域网由服务器，工作站，网络操作系统和中间设备组成。
MAC 地址	MAC 地址是烧录在硬件适配器上的一串唯一的序列号。
MTU （最大传输单元）	MTU （最大传输单元）是能够在网络中传输的最大的桢长度。如果有任何桢的长度大于 MTU 值，那就会被分割成较小的块。
NAT （网络地址转换）	NAT （网络地址转换）使得机构只使用一个地址出现在 Internet 上。NAT 转换每一个内部局域网的地址到一个 Internet 的公网地址 （反之亦然）。NAT 还能够提供一定的安全性，就好像防火墙一样让私有的网络隐藏在 WAN 接口的后面。
网络管理员	网络管理员是能够在机构中管理局域网的人。管理员的工作包括保证网络的安全，维护软硬件和韧件的更新，以及审计网络活动。
NTP （网络时间协议）	NTP （网络时间协议）用于同步计算机的时钟。Internet 主副服务器与协调世界时 （UTC）进行同步。
数据包	数据包是在网络中传输数据的一部分。数据包有时叫做桢和数据报。数据包不仅仅包含数据，还包含 IP 地址。
Ping	Ping （数据包 Internet 探测）是一种用于找出指定的 IP 地址是否在线的工具，通常用于网络调试。
接口	接口是计算机和网络设备进行通讯的进出路径。大多数的计算机有串口和并口，可以连接诸如打印机和调制解调器等设备。所有网络适配器都有接口，用于连接网线。
PPPoE （以太网上的点对点协议）	PPPoE （以太网上的点对点协议）用于在以太网上运行 PPP 协议。（通常用于拨号 Internet 连接）
协议	协议就是数据通讯的规则。
RIP （路由信息协议）	RIP （路由信息协议）是一种集成在 TCP/IP 协议中的路由协议。RIP 基于最小跳数在数据包的源和目的地寻找路由。
RTS （请求发送）	RTS （请求发送）是一个从传送站到接收站进行请求传输数据许可的信号。
服务器	服务器通常是功能强大和运算迅速的计算机，能够存储程序和数据。这些程序和数据共享给网络上的客户端和工作站。
SMTP （简单邮件传输协议）	SMTP （简单邮件传输协议）是标准的 Internet 电子邮件协议。SMTP 是一个 TCP/IP 协议，其定义了消息的格式并且包含了存储转发邮件的消息传输代理。
SNMP （简单网络管理协议）	SNMP （简单网络管理协议）是广泛用于网络监控和控制的协议。SNMP 硬件或软件组件传输网络设备活动数据到工作站，用于监控网络。
SSID （服务集标示符）	SSID （服务集标示符）是一种用于无线局域网的网络名。SSID 能够在无线局域网中发送的数据包中附加唯一的标识符。当设备试图接入无线局域网的时候，这个标识符充当了密码的功用。因为 SSID 能够区分一个无线局域网，接入点和无线设备如果要连接无线局域网就必须要有相同的 SSID。

术语	定义
子网掩码	子网掩码是用于在 IP 地址中指出网络位和主机位的。一个子网掩码存储在客户端，服务器或路由器中与入站的 IP 地址比对，以决定是否接受该数据包。
SysLog 服务器	SysLog 服务器监控 Syslog 消息并对其进行解码。
TCP （传输控制协议）	TCP （传输控制协议）是 TCP/IP 传输层的协议，能够确保网络上传输消息的正确性和完整性。
TCP/IP （传输控制协议 / Internet 协议）	TCP/IP （传输控制协议 /Internet 协议）是主要的 Internet 通讯协议。TCP 的部分能够确保数据完整地传送和接收。TCP/IP 协议簇的另一部分 UDP 可以用于发送对正确性和完整性要求不高的数据，例如实时视频和语音传输。
Telnet	Telnet 是虚拟终端协议，用于 Internet 和基于 TCP/IP 的网络。 Windows Telnet 客户端 Telnet 是用于连接远程设备并执行程序。Telnet 是 TCP/IP 通讯协议的集成组件。
UDP （用户报文协议）	UDP （用户报文协议）是 TCP/IP 协议簇中的一个协议，用于在对传输正确性要求不高的网络中传输信息，例如实时视频和音频，没有时间重新传输数据的时候就会丢弃。
虚拟服务器	虚拟服务器是与其他虚拟服务器 （例如，非专业服务器）共享资源的客户端服务器 （例如 Web 服务器）
WEP （有线对等加密）	WEP （有线对等加密）是无线局域网的安全协议，能够给无线网络提供和有线网络相等的加密安全。
WLAN （无线局域网）	WLAN （无线局域网）是无线通讯用于传输数据的网络。通常传输在 2.4GHz 频带上。WLAN 设备不需要像红外线设备相互对齐才能通讯。WLAN 设备使用连接到有线局域网的接入点可以连接到局域网。WLAN 设备的无线频率足够穿过非金属的墙壁和物体，能够覆盖大约一千英尺。笔记本电脑通过 PCMCIA 卡使用 WLAN，台式机通过无线网卡使用 WLAN。
WAN （广域网）	WAN （广域网）是能够覆盖广大地理范围的通讯网，例如一个国家。（和局域网相反，其只能覆盖一个小型区域，例如公司大楼）

保修

有限保修

感谢您购买 Billion 的产品。

盛达电业股份有限公司（下文简称为 Billion）提供 12 个月的产品硬件保修，其保修范围是在正常使用和正常服务下的材料缺损和工艺缺陷。关于产品的正常性能，在指定包装中的其他产品和 / 或 Billion 的用户手册中提供有限的保修。

Billion 不保修由于意外事故，不当使用，拆卸更改，错误安装，雷击，没有按照 Billion 得指导移除或修复序列号，或其他 Billion 先前指定的事件而引起的缺损或故障。此保修不包含正常磨损造成的缺损，不包含使用任何与本地、区域或国家技术或安全标准相违背的应用造成的损失。

产品中的标准软件是在“照原来的样子”的条件下提供的。Billion 不保证软件没有缺陷。提供的软件可能不能适合终端用户特定的使用。

若要享受保修服务，产品必须报告给 Billion，Billion 授权的当地代理商或 Billion 授权的分销商，从他们那里获得设备保修的信息。

若要享受保修服务，技术支持或客户服务，请联系 Billion 授权的当地代理商或 Billion 授权的分销商。在任何情况下，我们都欢迎通过下面的方式联系 Billion 总部：

E-mail：support@billion.com
主页：http://cn.billion.com